เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Policy)
สำนักงานเศรษฐกิจการคลัง
พ.ศ. ๒๕๖๘

สารบัญ

หน้า

คำนำ ๕
หลักการและเหตุผล ๖
๑. วัตถุประสงค์ (Objective) ๗
๒. การประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๗
๓. การสร้างความตระหนักรู้ ๗
๔. ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๘
๕. การบังคับใช้ (Enforcement) ๘
๖. กระบวนการทางวินัย ๘
๗. นิยาม (Define) ๘

หมวดที่ ๑ แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๑
๘. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ๑๑
๙. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) ๑๒
๑๐. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) ๑๓
๑๑. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ๑๓
๑๒. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) ๑๒

หมวดที่ ๒ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและระบบเครือข่ายสำหรับผู้ใช้งาน ๑๕
๑๓. นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy) ๑๕
๑๔. นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy) ๑๖
๑๕. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy) ๒๐
๑๖. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) ๒๑
๑๗. นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) ๒๑
๑๘. นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy) ๒๒
๑๙. นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy) ๒๓
๒๐. นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy) ๒๔
๒๑. นโยบายการบริหารจัดการบันทึก (Records Management Policy) ๒๕
๒๒. นโยบายการเก็บรักษาและลบทำลายข้อมูล (Data Retention and Disposal Policy) ๒๖
๒๓. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ๒๖

สารบัญ (ต่อ)

หน้า

หมวดที่ ๓ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและระบบเครือข่ายสำหรับผู้ดูแลระบบ ๒๘
๒๔. นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security) ๒๘
๒๕. นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy) ๓๓
๒๖. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy) ๔๖
๒๗. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) ๕๒
๒๘. นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) ๕๔
๒๙. นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy) ๕๕
๓๐. นโยบายการบริหารจัดการความต่อเนื่องของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management Policy) ๕๖
๓๑. นโยบายความมั่นคงปลอดภัยด้านบุคลากร (Human Security Policy) ๕๘
๓๒. นโยบายการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (Project Management Policy) ๖๐
๓๓. นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy) ๖๐
๓๔. นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy) ๖๖
๓๕. นโยบายด้านการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management Policy & Procedure) ๖๘
๓๖. นโยบายความมั่นคงปลอดภัยด้านบริการที่ได้รับจากผู้ให้บริการ (Supplier Relationships Policy) ๗๖
๓๗. นโยบายการปฏิบัติตามกฎหมาย มาตรฐาน และข้อบังคับ (Compliance Policy) ๗๙
๓๘. นโยบายการใช้บริการคลาวด์ (Cloud Services Policy) ๘๑
๓๙. นโยบายการบริหารจัดการบันทึก (Records Management Policy) ๘๒
๔๐. นโยบายการบริหารจัดการช่องโหว่ (Vulnerability Management Policy) ๘๓
๔๑. นโยบายการบริหารจัดการการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logging Policy) ๘๔
๔๒. นโยบายการเก็บรักษาและลบทำลายข้อมูล (Data Retention and Disposal Policy) ๘๕
๔๓. นโยบายการกำหนดค่า Configuration อย่างมั่นคงปลอดภัย ๘๗
๔๔. นโยบายการป้องกันข้อมูลรั่วไหล ๘๘

หมวดที่ ๔ แนวปฏิบัติในการใช้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพามาใช้งานระบบเทคโนโลยีสารสนเทศ ๙๑
๔๕ แนวปฏิบัติในการใช้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพามาใช้งานระบบเทคโนโลยีสารสนเทศ ๙๑

สารบัญ (ต่อ)

หมวดที่ ๕ แนวปฏิบัติในการรักษาความปลอดภัยข้อมูลส่วนบุคคลสำหรับการใช้งานระบบอินทราเน็ต (Intranet) ของ สศค. ๙๗

๔๖ แนวปฏิบัติในการรักษาความปลอดภัยข้อมูลส่วนบุคคลสำหรับการใช้งานระบบอินทราเน็ต (Intranet) ของ สศค. ๙๗

หมวดที่ ๖ แนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๑๐๗

๔๗ แนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๑๐๗

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือและปัจจัยที่สำคัญที่ช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยลดต้นทุนในการดำเนินงานด้านต่าง ๆ ให้แก่หน่วยงานที่มีการเชื่อมต่อระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายทางอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสาร เป็นต้น แม้ว่าระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และสามารถช่วยอำนวยความสะดวกในด้านต่าง ๆ แต่ในขณะเดียวกันก็มีความเสี่ยงที่สูงและอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เนื่องจากการใช้งานระบบเทคโนโลยีสารสนเทศอาจจำเป็นต้องติดต่อเชื่อมโยงข้อมูลไปยังหน่วยงานอื่นทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลากหลายรูปแบบ เช่น โปรแกรมประสงค์ร้ายหรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ตเพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการเพื่อเรียกค่าไถ่หรือการนำไปใช้ผิดวัตถุประสงค์ ซึ่งเหตุการณ์ต่าง ๆ เหล่านี้เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมากและทำให้สูญเสียชื่อเสียงหรือภาพลักษณ์ของหน่วยงาน ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงจำเป็นต้องตระหนักถึงการให้การดูแลบำรุงรักษาและการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

สำนักงานเศรษฐกิจการคลัง (สศค.) จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) สศค. ปี พ.ศ. ๒๕๖๘ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ รวมถึงสอดคล้องตามข้อกำหนดของกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจากทุกหน่วย ภายใน สศค. อย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ ตลอดจนมีการทบทวนและปรับปรุงเพื่อให้สอดคล้องตามข้อกำหนดของกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องรวมถึงการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว สศค. จึงหวังเป็นอย่างยิ่งว่า แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของ สศค. ทุกคนในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สศค. ต่อไป

สำนักงานเศรษฐกิจการคลัง
กันยายน ๒๕๖๘

หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่ให้ความคุ้มครองข้อมูลส่วนบุคคลและสิทธิ์ของเจ้าของข้อมูลส่วนบุคคล ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ สศค. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ สศค. จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

/๑. วัตถุประสงค์ ...

๑. วัตถุประสงค์ (Objective)

๑.๑ เพื่อรักษาซึ่งความมั่นคงปลอดภัยของสารสนเทศ ประกอบด้วย การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

๑.๒ เพื่อกำหนดทิศทางการบริหารจัดการ แนวทางปฏิบัติและข้อปฏิบัติในการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับข้อกำหนดของกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

๑.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติให้แก่บุคลากรของ สศค. เจ้าหน้าที่ และผู้ดูแลระบบสารสนเทศและระบบเครือข่าย รวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับ สศค. ตลอดจนตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของ สศค. ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๔ เพื่อให้มีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญเกิดขึ้น

๒. การประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติได้ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

๒.๑ หนังสือเวียนภายใน สศค.

๒.๒ หนังสือเวียนภายนอก สศค.

๒.๓ เว็บไซต์ของ สศค.

๒.๔ ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) ของ สศค.

๒.๕ ระบบลงนามรับทราบทางออนไลน์ของ สศค.

๓. การสร้างความตระหนักรู้

การสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) มีแนวปฏิบัติดังนี้

๓.๑ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

สร้างความรู้ความเข้าใจ วิธีการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์อย่างมั่นคงปลอดภัยให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักรู้ ความเข้าใจถึงภัยและผลกระทบ รวมถึงการป้องกันการกระทำผิดจากการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกันตามความเหมาะสม มีข้อปฏิบัติดังนี้

๓.๑.๑ ประกาศหรือเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สศค.

๓.๑.๒ จัดฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศอย่างไม่ถูกต้องหรือไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

/๓.๒.๓ จัดฝึกอบรม ...

๓.๒.๓ จัดฝึกอบรมการใช้งานระบบสารสนเทศของ สศค. อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการพัฒนาระบบสารสนเทศขึ้นมาใช้งาน หรือมีการปรับปรุง/ปรับเปลี่ยนการใช้งานของระบบสารสนเทศ

๓.๒.๔ จัดทำคู่มือการใช้งานระบบสารสนเทศเผยแพร่บนระบบสารสนเทศ หรือทางเว็บไซต์ของ สศค.

๓.๒.๕ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สศค. รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้องให้แก่บุคลากรของ สศค. อย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาจากแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของ สศค.

๓.๒.๖ จัดสัมมนาเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยอาจจัดร่วมกับการสัมมนาหรือการอบรมด้านอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้

๓.๒.๗ จัดทำสื่อประชาสัมพันธ์เพื่อให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่สม่ำเสมอ

๓.๒.๘ การกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งานเพื่อสร้างการมีส่วนร่วมและลงสู่ภาคปฏิบัติ

๔. ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่ สศค. หรือผู้ใดผู้หนึ่งอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของ สศค. (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

๕. การบังคับใช้ (Enforcement)

บังคับใช้กับบุคลากรของ สศค. ทุกระดับ เจ้าหน้าที่ ผู้ดูแลระบบสารสนเทศและระบบเครือข่าย รวมถึงผู้ให้บริการภายนอกที่อยู่ในขอบเขตระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของ สศค.

๖. กระบวนการทางวินัย

๖.๑ ผู้ก่อเหตุละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ สศค. ทั้งที่เป็นบุคลากรของ สศค. หรือผู้ให้บริการภายนอกที่จะเข้ามาดำเนินการใด ๆ ร่วมกับ สศค. ต้องได้รับการพิจารณาโทษตามกระบวนการลงโทษทางวินัยของ สศค. โดยอ้างอิงกระบวนการพิจารณาลงโทษทางวินัยของฝ่ายทรัพยากรบุคคล

๖.๒ ก่อนพิจารณาดำเนินการลงโทษทางวินัยต่อบุคลากรของ สศค. หรือผู้ให้บริการภายนอกที่จะเข้ามาดำเนินการใด ๆ ร่วมกับ สศค. ต้องมีหลักฐานการก่อเหตุละเมิดด้านความมั่นคงปลอดภัยสารสนเทศที่ชัดเจนและเชื่อถือได้ก่อนการพิจารณาเสมอ

๗. นิยาม (Define)

๗.๑ “ผู้ใช้งาน” หมายความว่า บุคลากรของ สศค. รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของ สศค.

/๗.๒ “ผู้ดูแลระบบ” ...

๗.๒ “ผู้ดูแลระบบ” หมายความว่า ผู้อำนวยการส่วนของศูนย์เทคโนโลยีสารสนเทศ เจ้าหน้าที่ผู้ปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้อำนวยการส่วนขึ้นไป ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแลรักษาระบบสารสนเทศ และระบบเครือข่ายที่ใช้งานอยู่ใน สศค. หรือหน่วยงานที่มีหน้าที่และรับผิดชอบในการดูแลระบบสารสนเทศ และระบบเครือข่ายโดยตรง

๗.๓ “สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผนผัง แผนที่ ภาพถ่าย ฟิล์ม การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๗.๔ “ระบบสารสนเทศ” หมายความว่า ระบบงานของ สศค. ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของ สศค.

๗.๕ “ระบบเครือข่าย” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ สศค. ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่น ๆ

๗.๖ “ทรัพย์สิน” หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับ สศค. ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อ สศค.

๗.๗ “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของ สศค. โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๗.๘ “สิทธิ์” หมายความว่า ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ปฏิบัติงาน และผู้ใช้งานที่เกี่ยวข้อง ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของ สศค.

๗.๙ “การเข้าถึง” หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

/๗.๑๐ “บัญชีผู้ใช้งาน” ...

๗.๑๐ “บัญชีผู้ใช้งาน” หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก

๗.๑๑ “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๗.๑๒ “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ซึ่งอาจทำให้ระบบของ สศค. ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๗.๑๓ “การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลและผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๗.๑๔ “การยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปโดยใช้ชื่อผู้ใช้และรหัสผ่าน

๗.๑๕ “SSL (Secure Socket Layer)” หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์ หรือ Application ที่ใช้งาน

๗.๑๖ “VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัวสำหรับผู้มีสิทธิ์ใช้ในการรับส่งข้อมูลจริงซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะโดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๗.๑๗ “ข้อมูลดิจิทัล (Digital Data)” หมายความว่า ข้อมูลที่แสดงอยู่ในรูปแบบที่เครื่องคอมพิวเตอร์และอุปกรณ์ดิจิทัลอื่น ๆ สามารถอ่านและประมวลผลได้

๗.๑๘ “สารสนเทศดิจิทัล” (Digital Information) หมายความว่า สารสนเทศดิจิทัล (Digital Information) ข้อมูลที่ถูกสร้าง จัดเก็บ ประมวลผล และส่งผ่านระบบอิเล็กทรอนิกส์.ข้อมูลเหล่านี้สามารถอยู่ในรูปแบบต่าง ๆ เช่น ข้อความ ภาพ เสียง วิดีโอ หรือข้อมูลดิจิทัลอื่น ๆ

/หมวดที่ ๑ ...

หมวดที่ ๑
แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สศค. ต้องกำหนด จัดทำ และมอบหมายผู้รับผิดชอบในการนำกรอบมาตรฐานตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปประยุกต์ใช้งาน ดังนี้

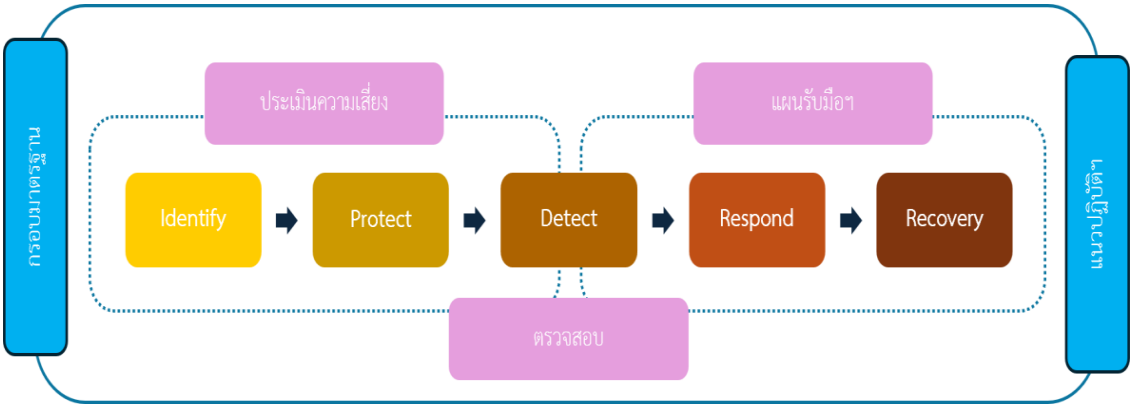
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)



๘. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

<u>วัตถุประสงค์</u>

เพื่อระบุความเสี่ยงที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศของ สศค. โดยพิจารณากำหนดแนวทางในการบริหารจัดการความเสี่ยงให้ครอบคลุมทรัพย์สินสารสนเทศของ สศค. อย่างเหมาะสม ดำเนินการดังนี้

๘.๑ การจัดการทรัพย์สิน (Asset Management) ให้ถือปฏิบัติตามนโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)

๘.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

/๘.๒.๑ ต้องประเมิน ...

๘.๒.๑ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ สศค. ตามขั้นตอนการบริหารความเสี่ยง (Risk Management Procedure)

๘.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ให้ถือปฏิบัติตามนโยบายการบริหารจัดการช่องโหว่ (Vulnerability Management Policy)

๘.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ให้ถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านบริการที่ได้รับจากผู้ให้บริการ (Supplier Relationships Policy)

๙. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับ สศค. อย่างมีประสิทธิภาพและประสิทธิผล

๙.๑ การควบคุมการเข้าถึง (Access Control) ให้ถือปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๙.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ให้ถือปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy) นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy) และนโยบายการกำหนดค่า Configuration อย่างมั่นคงปลอดภัย

๙.๓ การเชื่อมต่อระยะไกล (Remote Connection) ให้ถือปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

๙.๔ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๙.๔.๑ ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับบุคลากรของ สศค. และผู้ให้บริการภายนอกที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ สร้างการตระหนักรู้ข้อกำหนดของกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๙.๔.๒ ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

/๑๐. มาตรการ ...

๑๐. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการตรวจสอบและเฝ้าระวังภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นกับ สศค.

๑๐.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๑๐.๑.๑ ต้องสร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของ สศค. วิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ให้ถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)Intrusion Prevention System Policy: IDS/IPS Policy)

๑๐.๑.๒ ต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ ๑๐.๑.๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๑๑. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการรับมือเมื่อเผชิญกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑๑.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๑๑.๑.๑ ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๑๑.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๑๑.๒.๑ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๑๑.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๑๑.๓.๑ มีการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ที่อาจจะเกิดขึ้น

ทั้งนี้ สศค. ได้มีการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) เพื่อเตรียมรับมือกับเหตุการณ์ด้านไซเบอร์ที่อาจจะเกิดขึ้น

/๑๒. มาตรการ ...

๑๒. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการรับมือหลังเผชิญกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรักษาและฟื้นฟูความเสียหายที่เกิดขึ้นจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑๒.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๑๒.๑.๑ ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) หรือแผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan: DRP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ สศค. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของ สศค. เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๑๒.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP หรือ DRP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ BCP หรือ DRP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

/หมวดที่ ๒ ...

หมวดที่ ๒
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและระบบเครือข่ายสำหรับผู้ใช้งาน

๑๓. นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของ สศค.

๑๓.๑ บุคลากรของ สศค. ต้องล็อค และปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแลเพื่อป้องกันทรัพย์สินของ สศค.

๑๓.๒ ไม่อนุญาตให้หน่วยงานภายนอกและบุคลากรที่ไม่มีกิจเข้าไปในพื้นที่สำคัญที่มีการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) หรือ Data Center เว้นแต่ได้รับการอนุญาต

๑๓.๓ หน่วยงานภายนอกและบุคลากรที่มีส่วนเกี่ยวข้อง หากต้องการเข้าพื้นที่รักษาความมั่นคงปลอดภัย ต้องให้ผู้ประสานงานขออนุญาตเข้าพื้นที่ล่วงหน้าอย่างน้อย ๑ วันทำการ โดยต้องแจ้งชื่อผู้ที่ต้องการเข้าพื้นที่ เหตุผลที่เพียงพอในการเข้าพื้นที่ และกำหนดเวลาในการเข้าพื้นที่

๑๓.๔ หน่วยงานภายนอกและบุคลากรที่มีส่วนเกี่ยวข้องต้องพิสูจน์ตัวตน โดยการใช้บัตรรูด และ/หรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า – ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) และต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการปฏิบัติงาน หรืออยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

๑๓.๕ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายเข้ามาภายใน สศค. จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๑๓.๖ การปฏิบัติงานในพื้นที่รักษาความมั่นคงปลอดภัย (Working in Secure Areas)

๑๓.๖.๑ ห้ามนำอาหาร น้ำ สิ่งที่เป็นอาหารของหนูและแมลง รวมถึงสิ่งที่อาจก่อให้เกิดฝุ่นละอองเข้ามาในพื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

๑๓.๖.๒ ห้ามบันทึกภาพนิ่งและภาพเคลื่อนไหวภายในพื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) เว้นแต่ความจำเป็นในการบำรุงรักษา

/๑๔. นโยบาย ...

๑๔. นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของ สศค. และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งสามารถตรวจสอบติดตาม พิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของ สศค. ได้อย่างถูกต้อง ตลอดจนป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑๔.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

กำหนดวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑๔.๑.๑ ผู้ใช้งาน และ/หรือ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศจะต้องได้รับอนุญาตจากเจ้าหน้าที่ผู้รับผิดชอบข้อมูลและระบบงานตามความจำเป็น โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๔.๑.๒ ไม่อนุญาตให้ผู้ใช้งานนำอุปกรณ์คอมพิวเตอร์แบบพกพา โทรศัพท์มือถือ หรืออุปกรณ์ประเภท Mobile device ส่วนตัวเข้าถึงระบบเทคโนโลยีสารสนเทศของ สศค. ยกเว้น ได้รับการอนุญาตเป็นกรณีไป ในกรณีได้รับอนุญาตให้ใช้งาน ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิ์ในการตรวจสอบ หรือเก็บรวบรวมหลักฐานจากอุปกรณ์ดังกล่าวเมื่อเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยสารสนเทศของ สศค.

๑๔.๑.๓ จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ โดยไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งโปรแกรมอรรถประโยชน์ อย่างไรก็ตาม ในกรณีที่มีความจำเป็น สามารถขออนุญาตผู้บังคับบัญชาในการติดตั้งโปรแกรมอรรถประโยชน์โดยชี้แจงเหตุผลและความจำเป็นก่อนดำเนินการติดตั้ง ทั้งนี้ เพื่อป้องกันการเพิ่มสิทธิ์โดยพละการของผู้ใช้งาน

๑๔.๑.๔ กำหนดเวลาเข้าถึงได้ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๑๔.๑.๕ ผู้ได้รับสิทธิ์ทำการ Log In ด้วย User (ชื่อผู้ใช้) และ Password (รหัสผ่าน) ผ่านระบบ Single Sign-On เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุดต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

๑๔.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ

๑๔.๒.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของ สศค.

/๑๔.๒.๒ ผู้ใช้งาน ...

๑๔.๒.๒ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของ สศค. ร่วมกัน

๑๔.๒.๓ ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๑๔.๒.๔ ผู้ใช้งานควรทำการล็อคหน้าจอ (Logout) ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๔.๓ ความรับผิดชอบของผู้ใช้งาน

๑๔.๓.๑ ผู้ใช้งานต้องได้รับบัญชีผู้ใช้สำหรับระบุตัวตนแบบ ๑ ต่อ ๑ เท่านั้น กรณีมีการใช้งานบัญชีผู้ใช้ร่วมกันต้องมีการระบุตัวแทนผู้รับผิดชอบการใช้งานบัญชีผู้ใช้งานนั้น ๆ

๑๔.๓.๒ ต้องใช้วิธีการพิสูจน์ตัวตนด้วยรหัสผ่านที่มีคุณภาพ หรือใช้วิธีการอื่นที่มีความมั่นคงปลอดภัยสูงกว่าในการพิสูจน์ตัวตนของผู้ใช้งานระบบปฏิบัติการ

๑๔.๔ แนวปฏิบัติที่ดีในการใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)

ศูนย์เทคโนโลยีสารสนเทศเป็นผู้บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุมและมีความมั่นคงปลอดภัย เนื่องจากรหัสผ่านเป็นวิธีพื้นฐานในการตรวจสอบตัวตนของผู้ใช้ระบบ ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่า ผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิ์เข้าสู่ระบบของ สศค. อย่างแท้จริง

๑๔.๔.๑ ผู้ใช้ระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนแก่บุคคลอื่น

๑๔.๔.๒ ผู้ใช้รายใหม่จะได้รับรหัสผ่านเริ่มแรก (รหัสผ่านชั่วคราว) ในการใช้ผ่านเข้าสู่ระบบในครั้งแรกและระบบต้องบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก ผู้ใช้สามารถสร้างรหัสผ่านที่มีคุณภาพและยากต่อการคาดเดา โดยใช้แนวปฏิบัติที่ดีในการสร้างรหัสผ่านที่มีคุณภาพ

๑๔.๔.๓ รหัสผ่านของผู้ใช้งานสำหรับการใช้งาน เช่น e-mail, Website, Desktop Computer, Notebook และระบบเทคโนโลยีสารสนเทศ เป็นต้น ควรเปลี่ยนเป็นประจำอย่างน้อยทุก ๖ เดือน ทั้งนี้แนะนำให้เปลี่ยนเป็นประจำทุก ๓ เดือน หรือเมื่อมีความเป็นไปได้ที่รหัสผ่านรั่วไหล เช่น ถูกโจมตีโดยไวรัสคอมพิวเตอร์ เป็นต้น

๑๔.๔.๔ ต้องเก็บรักษารหัสผ่านไว้ในที่ปลอดภัย ถือเป็นความลับ ไม่เปิดเผยรหัสผ่านให้ผู้อื่นล่วงรู้ หลีกเลี่ยงการบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกลงในกระดาษ หรือในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ ยกเว้นกรณีเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

/๑๔.๔.๕ ไม่เก็บรหัส ...

๑๔.๔.๕ ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ หรือโปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Saved Password) สำหรับเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองอยู่ รวมถึงไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๑๔.๔.๖ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

๑๔.๔.๗ ไม่ใช้รหัสผ่านเดียวกันในกรณีปฏิบัติงานและใช้ส่วนตัว

๑๔.๔.๘ ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องจดจำรหัสผ่านหลายตัว ควรใช้รหัสผ่านเดียวกันที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๑๔.๔.๙ ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

๑๔.๔.๑๐ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน หากเกิดกรณีรหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่โดยทันที ยกเว้นกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงานหลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๑๔.๔.๑๑ เมื่อเจ้าหน้าที่ของสำนักงาน/กอง/กลุ่ม/ศูนย์ ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้สำนักงาน/กอง/กลุ่ม/ศูนย์แจ้งศูนย์เทคโนโลยีสารสนเทศทันทีเพื่อดำเนินการเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ของผู้ที่ลาออกออกจากระบบทันทีที่ได้รับแจ้ง

๑๔.๔.๑๒ เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิ์พิเศษ ต้องได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการเวียนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๑๔.๔.๑๓ กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๑๔.๔.๑๔ เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๑๔.๔.๑๕ แนวปฏิบัติที่ดีในการสร้างรหัสผ่านที่มีคุณภาพ

(๑) กำหนดรหัสผ่านที่ง่ายต่อการจดจำเฉพาะตน แต่ต้องไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่าย ได้แก่ ชื่อ นามสกุล หมายเลขโทรศัพท์ และวันเกิด เป็นต้น หรือ ชื่อ นามสกุลของบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน

(๒) รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการประสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๓) รหัสผ่านต้องไม่มีคำซ้ำหรือตัวอักษรซ้ำ ต้องไม่เป็นตัวเลขทั้งหมด หรือตัวอักษรทั้งหมด

/(๔) การตั้งรหัส ...

(๔) การตั้งรหัสผ่านควรหลีกเลี่ยงการใช้ข้อมูลที่เกี่ยวข้องกับ สศค. ข้อมูลส่วนตัว ได้แก่ ชื่อ นามสกุล นามแฝง วันเดือนปีเกิด ที่อยู่ ทะเบียนยานพาหนะ หมายเลขโทรศัพท์ เลขที่บัตรประชาชน เลขที่บัตรประกันสังคม รหัสบัตรต่าง ๆ ชื่อบุคคลในครอบครัว เป็นต้น รวมถึงต้องไม่ใช้ชื่อภาพยนตร์ ชื่อสถานที่หรือชื่อสิ่งลึกลับ ศัพท์ที่มาจากพจนานุกรม เนื่องจากข้อมูลต่าง ๆ เหล่านี้ ง่ายต่อการคาดเดาของผู้โจมตีระบบ (Hackers)

(๕) การตั้งรหัสผ่าน ควรมีส่วนประกอบของอักษร อักขระพิเศษ และ/หรือ ตัวเลข ที่ประสมกันตามลักษณะดังต่อไปนี้

- ความยาวอย่างน้อย ๘ ตัวอักษรหรือตามที่ผู้บริหารจัดการระบบกำหนด
- อักษรตัวพิมพ์ใหญ่ ได้แก่ A, B, C, ... เป็นต้น
- อักษรตัวพิมพ์เล็ก ได้แก่ a, b, c, ... เป็นต้น
- ตัวเลข ได้แก่ ๐, ๑, ๒, ... เป็นต้น
- สัญลักษณ์พิเศษ ได้แก่ !, @, #, $, ... เป็นต้น

๑๔.๔.๑๖ กรณีมีการแอบอ้างรหัสผ่านหรือนำรหัสผ่านไปใช้โดยไม่ได้รับอนุญาตให้ผู้ใช้งานรีบดำเนินการแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที เพื่อระงับการใช้รหัสผ่านดังกล่าว หรือมีปัญหาการใช้งาน กรณีลืมชื่อผู้ใช้หรือรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ

๑๔.๔.๑๗ พึงระลึกเสมอว่า ความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศของ สศค. ที่ตนเองรับผิดชอบอยู่นั้น มีความสำคัญต่อตนและ สศค. เป็นอย่างยิ่ง ต้องไม่ให้ผู้อื่นบุกรุก แอบอ้าง หรือนำไปใช้ในทางที่ผิด เพราะอาจก่อให้เกิดผลเสียหายเป็นวงกว้างต่องานของตนเองและของ สศค.

๑๔.๕ การเข้ารหัสข้อมูล (Cryptography)

๑๔.๕.๑ ผู้ใช้งานต้องมีการเข้ารหัสข้อมูลสำหรับการส่งข้อมูลระหว่างหน่วยงานตามระดับชั้นของข้อมูลและสารสนเทศ โดยพิจารณาเลือกใช้อัลกอริทึมที่มีความแข็งแกร่ง น่าเชื่อถือและเหมาะสมกับระดับชั้นของข้อมูลและสารสนเทศ

๑๔.๕.๒ ผู้ใช้งานต้องเข้ารหัสข้อมูลซึ่งบันทึกไว้ในสื่อบันทึกที่สามารถเคลื่อนย้ายได้ เพื่อป้องกันการเข้าถึงข้อมูลให้มีความเหมาะสมตามระดับชั้นข้อมูล

๑๔.๘.๓ ผู้ใช้งานต้องดูแลรักษาอุปกรณ์ที่ใช้ในการพิสูจน์ตัวตนไม่ให้สูญหายหรือตกไปอยู่ในมือผู้อื่นที่ไม่มีหน้าที่ดูแลรับผิดชอบ และส่งคืนเมื่อสิ้นสุดการจ้างงาน

/๑๕. นโยบาย ...

๑๕. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้มีความปลอดภัยจากระบบภายนอก เป็นการป้องกันทรัพยากรและข้อมูลของ สศค. ให้มีการรักษาความลับ ความถูกต้อง และมีความพร้อมใช้งานของข้อมูลอยู่เสมอ

๑๕.๑ หากผู้ใช้งานต้องการนำอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของ สศค. ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๑๕.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๑๕.๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่ สศค. รับผิดชอบอยู่ ผู้ใช้งานจะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้บริการอื่น ๆ

๑๕.๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบเครือข่าย (Network System Administrator)

๑๕.๕ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของ สศค. จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑๕.๖ ผู้เข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของ สศค. ต้องผ่านการพิสูจน์ตัวตนจากระบบของ สศค. และจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ สศค. โดยผ่านความเห็นชอบจากผู้บังคับบัญชา (เลขานุการกรม/ผู้อำนวยการกอง/กลุ่ม/ศูนย์)

/๑๖. นโยบาย ...

๑๖. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๑๖.๑ ผู้ใช้งานต้องลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศตามความจำเป็นในการใช้งาน

๑๖.๒ ห้ามผู้ใช้งานนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองใน สศค. ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๑๖.๓ ห้ามผู้ใช้งานเปิด ad-hoc หรือ peer-to-peer Network

๑๗. นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่าง ๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานมีสิทธิ์ในการเข้าถึงการใช้งานไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน สศค.

๑๗.๑ ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการพิสูจน์ตัวตนทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User Account) และรหัสผ่าน (Password)

๑๗.๒ กำหนดนโยบายการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายโดยจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทาง สศค. อนุญาตให้ใช้งานเท่านั้น หากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน

๑๗.๓ สศค. มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของ สศค. หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายจนกว่าจะได้รับการแก้ไข

๑๗.๔ ภายหลังการอนุญาตให้ใช้งาน หากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของ สศค. หรือกฎหมาย หรืออาจทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของ สศค. ศูนย์เทคโนโลยีสารสนเทศสงวนสิทธิ์ในการยกเลิกการให้บริการทันที

/๑๘. นโยบาย ...

๑๘. นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผ่านระบบเครือข่ายของ สศค. ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้และไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่อาจจะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด

๑๘.๑ ผู้ใช้งานที่ต้องการใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของ สศค. จำเป็นต้องทำการลงทะเบียนบัญชีผู้ใช้งาน โดยกรอกข้อมูลคำขอเข้าใช้บริการและยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อดำเนินการกำหนดสิทธิ์ชื่อผู้ใช้งานรายใหม่และรหัสผ่าน (Username and Password)

๑๘.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที

๑๘.๓ เก็บรักษา Username and Password เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง และปฏิบัติตามแนวปฏิบัติที่ดีในการใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password) ที่ได้กำหนดไว้อย่างเคร่งครัด เช่น ไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือเก็บไว้ในสถานที่ที่สังเกตได้ เปลี่ยนรหัสผ่านทุก ๓ - ๖ เดือน เป็นต้น

๑๘.๔ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของ e-mail และให้ถือว่าเจ้าของ e-mail นั้นเป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ใน e-mail ของตน

๑๘.๕ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการหรือตามภารกิจของ สศค. ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ สศค. เพื่อติดต่องานของราชการเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ สศค. ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๑๘.๖ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๑๘.๗ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของ สศค. หรือก่อให้เกิดความเสียหาย

/๑๘.๙ พึงระมัดระวัง ...

๑๘.๙ พึงระมัดระวังการใช้ e-mail เพื่อไม่ให้เกิดความเสียหายต่อ สศค. หรือละเมิดลิขสิทธิ์ รบกวน หรือสร้างความน่ารำคาญ เผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดซึ่งมีลักษณะขัดหรือละเมิดต่อศีลธรรม ความมั่นคงของประเทศ ผิดกฎหมาย หรือกระทบต่อการดำเนินงานของ สศค. และแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ e-mail ผ่านระบบเครือข่ายของ สศค.

๑๘.๑๐ ไม่ระบุความสำคัญของข้อมูลลงบนหัวข้อไปรษณีย์อิเล็กทรอนิกส์ กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ

๑๘.๑๑ การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน ๑๕ เมกะไบท์

๑๘.๑๒ ตรวจสอบไฟล์เอกสารแนบที่มาจาก e-mail โดยใช้โปรแกรมป้องกันไวรัสทุกครั้งก่อนเปิดไฟล์ที่เป็น Executable File (ไฟล์นามสกุล .exe, .com)

๑๘.๑๓ ไม่เปิดหรือส่งต่อ e-mail หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๘.๑๔ ตรวจสอบ e-mail ของตนเองทุกวัน จัดเก็บแฟ้มข้อมูลและ e-mail ของตนให้เหลือจำนวนน้อยที่สุด และลบ e-mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้พื้นที่ในระบบ

๑๘.๑๕ หลังจากการใช้งาน e-mail เสร็จสิ้น ต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานไปรษณีย์อิเล็กทรอนิกส์ของตน

๑๙. นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของ สศค. ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์ (Social Network: LINE, Facebook, Twitter) ต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้และไม่ละเมิดสิทธิ์กระทำการใด ๆ ที่อาจจะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัดเพื่อให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๑๙.๑ ผู้ใช้งานที่ต้องการใช้ระบบอินเทอร์เน็ตของ สศค. จำเป็นต้องทำการลงทะเบียนบัญชีผู้ใช้งาน โดยกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของ สศค. โดยยื่นคำขอกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ สศค. โดยผู้ใช้งานต้องเป็นบุคลากรสังกัด สศค. สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๑๙.๒ ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตของ สศค. เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายกับ สศค.

/๑๙.๓ พึงใช้ ...

๑๙.๓ พึงใช้ข้อความที่สุภาพตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๑๙.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๑๙.๕ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน และห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สศค. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๙.๖ ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

๑๙.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและข้อมูลที่เป็นความลับของ สศค. ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ สศค. การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑๙.๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์ที่ใช้งาน และออกจากการเชื่อมต่อด้วยการ Logout จากการ Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑๙.๙ ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อย่างเคร่งครัด

๑๙.๑๐ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ (Social Network: LINE, Facebook, Twitter) ในรูปแบบและลักษณะตามที่ สศค. ได้กำหนดไว้เท่านั้น

๑๙.๑๑ ต้องตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับ สศค. จากการใช้งานเครือข่ายสังคมออนไลน์ ต้องแจ้งต่อศูนย์เทคโนโลยีสารสนเทศโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๒๐. นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางในการบริหารจัดการทรัพย์สินสารสนเทศในขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตั้งแต่การลงทะเบียนทรัพย์สิน ระบุหน้าที่ความรับผิดชอบอย่างเหมาะสม การป้องกันข้อมูลและสารสนเทศตามระดับที่กำหนดไว้ให้สอดคล้องกับระดับความสำคัญของทรัพย์สินนั้น ๆ รวมถึงมีการป้องกันการเปิดเผย แก้ไข เคลื่อนย้ายหรือกำจัดข้อมูลและสารสนเทศที่เก็บไว้ในสื่อบันทึกโดยไม่ได้รับอนุญาต

๒๐.๑ หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศของ สศค.

๒๐.๑.๑ ทรัพย์สินสารสนเทศของ สศค. ต้องถูกใช้งานเพื่อการดำเนินภารกิจของ สศค. เท่านั้น การใช้งานทรัพย์สินสารสนเทศของ สศค. เพื่อวัตถุประสงค์อื่นไม่สามารถกระทำได้

/๒๐.๑.๒ การใช้ ...

๒๐.๑.๒ การใช้งานทรัพย์สินสารสนเทศของ สศค. ต้องไม่ขัดกับข้อกำหนดของกฎหมายที่เกี่ยวข้องกับทรัพย์สินนั้น ๆ

๒๐.๑.๓ สศค. สงวนสิทธิ์ในการจัดเก็บข้อมูล การมอบสิทธิ์การใช้งานทรัพย์สินสารสนเทศให้แก่บุคลากรของ สศค. และบุคคลภายนอก หากเกิดเหตุละเมิดนโยบายหรือกฎหมายเนื่องจากการใช้งานทรัพย์สินสารสนเทศนั้น ๆ ไม่ว่าจะกระทำโดยผู้ได้รับมอบสิทธิ์หรือไม่ก็ตาม บุคลากรของ สศค. หรือบุคคลภายนอกที่เป็นผู้ได้รับมอบสิทธิ์การใช้งานจะไม่สามารถปฏิเสธความรับผิดชอบได้ ยกเว้นกรณีที่เหตุละเมิดนั้นมีสาเหตุจากความผิดพลาดในการบริหารความมั่นคงปลอดภัยสารสนเทศของ สศค. เอง หรือกรณีที่สามารถพิสูจน์ได้แน่ชัดว่าเป็นการกระทำโดยบุคคลอื่น

๒๐.๑.๔ บุคลากรของ สศค. และบุคคลภายนอกต้องแจ้งเหตุละเมิดความมั่นคงปลอดภัยที่เกิดขึ้นกับทรัพย์สินสารสนเทศที่ตนได้รับสิทธิ์ใช้งานทันทีที่พบต่อเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ

๒๐.๑.๕ สศค. สงวนสิทธิ์ในการจัดเก็บข้อมูลการใช้งานทรัพย์สินสารสนเทศรวมถึงการทบทวนและตรวจสอบการใช้งานทรัพย์สินสารสนเทศภายในขอบเขตที่กฎหมายอนุญาต

๒๐.๑.๖ บุคลากรของ สศค. คู่สัญญา หรือผู้ให้บริการภายนอกต้องคืนทรัพย์สินของ สศค. ที่ได้รับไปเพื่อการปฏิบัติงานเมื่อการจ้างงานสิ้นสุดลง

๒๐.๑.๗ หัวหน้างานหรือผู้ควบคุมการทำงานของบุคลากรนั้น ๆ ต้องควบคุมให้บุคลากรที่การจ้างงานใกล้จะสิ้นสุดลง ถ่ายโอนข้อมูลที่เกี่ยวข้องกับการทำงานทั้งหมดและข้อมูลที่ถือเป็นทรัพย์สินของ สศค. คืนอย่างครบถ้วน

๒๑. นโยบายการบริหารจัดการบันทึก (Records Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการป้องกันบันทึกไม่ให้สูญหาย ถูกทำลาย ปลอมแปลง หรือมีการเข้าถึงโดยไม่ได้รับอนุญาตและปล่อยออกไปโดยไม่ได้รับอนุญาต

๒๑.๑ ผู้ใช้งานต้องเก็บรักษาบันทึกต่าง ๆ ตามระยะเวลาในการเก็บบันทึกที่ สศค. กำหนด หรือกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

๒๑.๒ ผู้ใช้งานต้องดำเนินการกับบันทึกให้เหมาะสมตามระดับชั้นความลับของข้อมูล และสารสนเทศตามที่ สศค. กำหนดไว้

๒๑.๓ ผู้ใช้งานต้องดำเนินการตามกระบวนการจัดเก็บบันทึกที่ สศค. กำหนด

๒๑.๔ ผู้ใช้งานควรพิจารณาสื่อที่นำมาใช้ในการเก็บบันทึกข้อมูลให้มีสภาพที่สมบูรณ์ พร้อมใช้งาน

/๒๒. นโยบาย ...

๒๒. นโยบายการเก็บรักษาและลบทำลายข้อมูล (Data Retention and Disposal Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการป้องกันข้อมูลสารสนเทศที่ใช้ในการดำเนินงานที่มีความละเอียดอ่อนถูกเข้าถึงหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต และเพื่อให้การดำเนินการกับข้อมูลสารสนเทศสอดคล้องกับสัญญา กฎระเบียบ ข้อบังคับ และ กฎหมาย

๒๒.๑ ควรลบ ทำลายข้อมูลที่มีความละเอียดอ่อนเมื่อใช้งานเสร็จสิ้น หรือเมื่อไม่มีความจำเป็นต้องใช้งาน

๒๒.๒ การลบสารสนเทศบนระบบแอปพลิเคชั่น หรือบริการต่าง ๆ ผู้ใช้งานควรเลือกวิธีการลบที่เหมาะสม เช่น บันทึกข้อมูลในสื่ออิเล็กทรอนิกส์ ใช้วิธีการลบด้วยการเขียนทับ หรือการเข้ารหัส เป็นต้น

๒๒.๓ ต้องใช้ซอฟต์แวร์ที่มีความน่าเชื่อถือ ปลอดภัย เพื่อให้มั่นใจว่าไม่สามารถกู้ข้อมูลกลับมาได้อีก

๒๒.๔ ควรใช้วิธีการลบ ทำลายที่เหมาะสมกับสื่อบันทึกข้อมูล เพื่อป้องกันข้อมูลรั่วไหล และการนำกลับมาใช้ใหม่ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลายข้อมูลและสื่อบันทึก ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๒๒.๕ กรณีที่จะนำอุปกรณ์ สื่อบันทึกต่าง ๆ ที่มีข้อมูลออกไปนอกพื้นที่ หรือส่งซ่อม ควรตรวจสอบและพิจารณามาตรการป้องกันข้อมูลสารสนเทศที่มีความละเอียดอ่อน เพื่อป้องกันข้อมูลสารสนเทศถูกเข้าถึง เปิดเผยโดยไม่ได้รับอนุญาต

๒๒.๖ ผู้ใช้งานควรเลือกวิธีการลบ ทำลายที่เหมาะสมกับระดับชั้นความลับของข้อมูล

๒๒.๗ ผู้ใช้งานต้องจัดเก็บบันทึกหลักฐานในการลบ ทำลายข้อมูลสารสนเทศ เพื่อใช้เป็นหลักฐานในกรณีที่ข้อมูลรั่วไหล และใช้เพื่อวิเคราะห์หาสาเหตุของเหตุการณ์ดังกล่าว

๒๓. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการป้องกันการเข้าถึงเอกสารและข้อมูลสำคัญทางกายภาพและทางหน้าจอแสดงผล

๒๓.๑ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security Of System Documentation)

๒๓.๑.๑ ไม่วางเอกสาร บันทึก สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ ฯลฯ ที่สำคัญ หรือที่มีความลับทิ้งไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

/๒๓.๑.๒ นำเอกสาร ...

๒๓.๑.๒ นำเอกสารออกจากเครื่องพิมพ์เอกสารทันทีที่พิมพ์งานเสร็จ

๒๓.๑.๓ บริหารจัดการเอกสาร บันทึก สื่อบันทึกข้อมูลตามนโยบายการบริหารจัดการบันทึกข้อมูล

๒๓.๑.๔ ทำลายเอกสาร บันทึก สื่อบันทึกข้อมูลตามแนวทางการทำลายข้อมูลและสื่อบันทึก

๒๓.๑.๕. เอกสาร บันทึก สื่อบันทึกข้อมูลที่มีความสำคัญ หรือที่มีความลับ ห้ามเคลื่อนย้ายโดยผู้ที่ไม่มีสิทธิ์ ให้ดำเนินการโดยเจ้าของข้อมูลเท่านั้น เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

๒๓.๑.๖ เอกสาร บันทึก สื่อบันทึกข้อมูลที่มีความสำคัญ หรือที่มีความลับ ต้องถูกจัดเก็บในตู้เอกสาร หรือโต๊ะทำงานที่สามารถควบคุมการเข้าถึงได้

๒๓.๑.๗ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๒๓.๑.๘ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

๒๓.๑.๙ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ (อินเทอร์เน็ต) เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๒๓.๒ มาตรการป้องกันหน้าจอคอมพิวเตอร์

๒๓.๒.๑ ระวัง ป้องกัน ควบคุม ผู้ที่ไม่ได้รับอนุญาตเห็นข้อมูลสารสนเทศที่แสดงผลผ่านทางหน้าจออุปกรณ์แสดงผล เช่น หน้าจอคอมพิวเตอร์ หน้าจอมือถือ หน้าจอเครื่องพิมพ์ เป็นต้น

๒๓.๒.๒ ลงชื่อออกจากระบบงานและระบบปฏิบัติการคอมพิวเตอร์ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๒๓.๒.๓ กำหนดระยะเวลาในการล็อกหน้าจอคอมพิวเตอร์เมื่อไม่มีการใช้งาน

๒๓.๒.๔ ไม่นำไฟล์ข้อมูลสำคัญมาแสดงบนหน้าจอคอมพิวเตอร์

๒๓.๒.๕ ไม่ติด Username และ/หรือ Password ไว้บนหน้าจอคอมพิวเตอร์ หรือบริเวณที่ผู้อื่นสามารถมองเห็นได้

/หมวดที่ ๓ ...

หมวดที่ ๓
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและระบบเครือข่ายสำหรับผู้ดูแลระบบ

๒๔. นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของ สศค. ตลอดจนผู้มาเยือน

๒๔.๑ การจัดการบริเวณล้อมรอบ (Physical Security Management) ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ใช้งานเฉพาะระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายให้ชัดเจน พื้นที่ให้บริการแก่ผู้ใช้งาน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน

๒๔.๑.๑ กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน โดยแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒๔.๑.๒ พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน (Data Center) ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

๒๔.๑.๓ มีระบบป้องกันการบุกรุกที่ติดตั้งครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๒๔.๑.๔ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้ได้ตามปกติ

๒๔.๒ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานเฉพาะระบบเทคโนโลยีสารสนเทศ

๒๔.๓ การควบคุมการเข้า - ออก (Physical Entry Controls) ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า - ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายให้ครอบคลุมเรื่องต่าง ๆ ดังนี้

๒๔.๓.๑ ให้มีการบันทึกวันและเวลาเข้า - ออก พื้นที่สำคัญของผู้มาเยือน (Visitors)

๒๔.๓.๒ ดูแลผู้มาเยือนในพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญจนเสร็จสิ้นภารกิจเพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๒๔.๓.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญ

๒๔.๓.๔ บุคคลภายนอกต้องแจ้งเหตุผลที่เพียงพอในการเข้าถึงบริเวณที่มีความสำคัญ

๒๔.๓.๕ สร้างความตระหนักให้ผู้มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์ หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญ

๒๔.๓.๖ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

/๒๔.๓.๗ ไม่อนุญาต ...

๒๔.๓.๗ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๒๔.๓.๘ มีการพิสูจน์ตัวตน โดยการใช้บัตรรูด และ/หรือการใช้รหัสผ่าน เพื่อควบคุมการเข้า – ออก ในพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญ (Data Center)

๒๔.๓.๙ จัดเก็บบันทึกการเข้า – ออก สำหรับพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบภายหลังเมื่อมีความจำเป็น

๒๔.๓.๑๐ เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการปฏิบัติงานภานในศูนย์เทคโนโลยีสารสนเทศ

๒๔.๓.๑๑ ผู้มาเยือนต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาที่อยู่ภายในศูนย์เทคโนโลยีสารสนเทศ

๒๔.๓.๑๒ ต้องจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญ

๒๔.๓.๑๓ จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่ใช้งานหรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๒๔.๓.๑๔ การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery and Loading Areas)

(๑) จำกัดการเข้าถึงพื้นที่ใช้งานหรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่ใช้งานหรือบริเวณส่งมอบนั้น

(๓) จัดพื้นที่หรือบริเวณที่ส่งมอบไว้เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายใน สศค.

(๔) ให้ตรวจสอบวัสดุหรือผลิตภัณฑ์ต่าง ๆ ที่อาจเป็นอันตรายก่อนที่จะเคลื่อนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๕) ลงทะเบียน ตรวจนับวัสดุหรือผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของ สศค.

๒๔.๔ มาตรการควบคุมความมั่นคงปลอดภัยที่ใช้ในพื้นที่ต้องเป็นไปตามข้อกำหนดของกฎหมายด้านการควบคุมอาคารและกฎหมายอื่นที่เกี่ยวข้อง

๒๔.๕ อุปกรณ์สำคัญต้องถูกติดตั้งในบริเวณที่ยากแก่การเข้าถึงจากบุคคลภายนอก และต้องล็อค และปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแลเพื่อป้องกันทรัพย์สินของ สศค.

๒๔.๖ ต้องไม่ระบุชื่อพื้นที่ใช้งานหรือข้อมูลอื่นที่สื่อให้บุคคลภายนอกทราบความสำคัญหรือกิจกรรมที่เกิดขึ้นในพื้นที่ใช้งาน เช่น ห้องคอมพิวเตอร์ Data Center ห้องเก็บเทปสำรองข้อมูลลงในป้ายห้อง ป้ายบอกทางในอาคาร และจุดอื่นที่บุคคลภายนอกสามารถเข้าถึงได้

๒๔.๗ แผนผังของพื้นที่ใช้งาน เบอร์ติดต่อภายใน และข้อมูลอื่นที่บ่งบอกที่ตั้งของอุปกรณ์สำคัญต้องถูกควบคุมให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

/๒๔.๘ ต้องมีการ ...

๒๔.๘ ต้องมีการป้องกันอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล เช่น ต้องล็อกหน้าจอเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องให้บริการทุกครั้งที่ไม่ใช้งาน และต้องมีการตั้งค่าอุปกรณ์ดังกล่าวให้มีการล็อกหน้าจออัตโนมัติเมื่อไม่มีผู้ใช้งาน เครื่องพิมพ์ที่ตั้งไว้และมีการ สั่งพิมพ์จากระยะไกลต้องมีการป้องกันการเข้าถึงเอกสารที่พิมพ์ออกมา

๒๔.๙ การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External End Environmental Threats)

๒๔.๙.๑ การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง Data Center ให้น้อยที่สุด

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

(๓) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในห้อง Data Center

(๔) ดำเนินการตรวจสอบ สอดส่องและดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว โดยมีการตรวจสอบระดับอุณหภูมิ ความชื้นว่าอยู่ในระดับปกติหรือไม่

๒๔.๙.๒ ห้ามนำวัตถุไวไฟ วัตถุมีพิษ และวัตถุอันตรายอื่นใดเข้ามาใกล้พื้นที่มั่นคงปลอดภัยเกินกว่าระยะปลอดภัย โดยพิจารณาตามความเหมาะสม

๒๔.๙.๓ ที่ตั้งของศูนย์สำรองต้องมีระยะห่างจาก สศค. เพียงพอที่จะไม่ได้รับผลกระทบจากภัยพิบัติขนาดใหญ่พร้อมกัน

๒๔.๙.๔ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) ต้องตั้งอยู่ในอาคารที่มั่นคงแข็งแรง สามารถทนต่อแรงลม แรงแผ่นดินไหว อย่างน้อยตามที่กฎหมายกำหนด

๒๔.๙.๕ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) ต้องตั้งอยู่ในระดับที่สูงเพียงพอที่จะไม่ได้รับผลกระทบจากภัยคุกคาม เช่น น้ำท่วม อุบัติเหตุจากรถยนต์

๒๔.๙.๖ ต้องติดตั้งระบบควบคุมเพลิงไหม้ที่เหมาะสมกับขนาดของพื้นที่และไม่เป็นอันตรายต่อบุคลากร อุปกรณ์ รวมถึงทรัพย์สินสำคัญที่อยู่ในพื้นที่มั่นคงปลอดภัย

/๒๔.๙.๗ ต้องติดตั้ง ...

๒๔.๙.๗ ต้องติดตั้งระบบตรวจจับและควบคุมภัยคุกคามจากสภาพแวดล้อม เช่น ระบบดับเพลิง ระบบตรวจจับน้ำรั่วที่เหมาะสมกับความต้องการของอุปกรณ์ที่ติดตั้งอยู่ในพื้นที่มั่นคงปลอดภัย

๒๔.๑๐ การปฏิบัติงานในพื้นที่รักษาความมั่นคงปลอดภัย (Working in Secure Areas)

๒๔.๑๐.๑ ห้ามแสดงรูปภาพ หรือข้อมูลสำคัญต่าง ๆ เช่น แผนผังระบบเครือข่าย และแผนผังของพื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

๒๔.๑๐.๒ การให้ข้อมูลแก่บุคคลภายนอกเพื่อประกอบการปฏิบัติงานต้องพิจารณาให้ข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงานตามหน้าที่ของบุคคลนั้น ๆ เท่านั้น

๒๔.๑๐.๓ ต้องทำการปิดล็อกตู้ Rack ตู้เอกสาร ตู้ไฟฟ้า และอุปกรณ์สำคัญอื่น ๆ ทันทีหลังจากใช้งานเสร็จ

๒๔.๑๐.๔ ห้ามเปิดประตูหรือช่องเปิดใด ๆ บริเวณผนังหรือกำแพงของพื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หรือพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) ค้างไว้โดยไม่มีเหตุอันควร และต้องตรวจสอบว่าประตูและช่องเปิดเหล่านั้นได้ถูกปิดล็อกอย่างถูกต้องเมื่อเสร็จสิ้นการปฏิบัติงาน

๒๔.๑๑ การจัดตั้ง และป้องกันอุปกรณ์ (Equipment Sitting and Protection)

๒๔.๑๑.๑ ต้องมีการจัดตั้ง จัดเก็บ และป้องกันอุปกรณ์เพื่อลดความเสี่ยงจากภัยคุกคาม อันตรายด้านสภาพแวดล้อมและโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงอุปกรณ์ที่มีความสำคัญต้องได้รับการป้องกันเป็นพิเศษ

๒๔.๑๑.๒ ต้องเฝ้าสังเกตสภาพแวดล้อมในพื้นที่ติดตั้งอุปกรณ์อย่างสม่ำเสมอ หากพบความผิดปกติต้องดำเนินการปรับปรุงให้สภาพแวดล้อมในพื้นที่ติดตั้งอุปกรณ์กลับมาเป็นปกติภายในระยะเวลาที่ไม่เป็นอันตรายกับอุปกรณ์ในพื้นที่นั้น

๒๔.๑๑.๓ ต้องใช้งานระบบและอุปกรณ์สนับสนุนตามข้อกำหนด และคำแนะนำของผู้ผลิตอุปกรณ์

๒๔.๑๑.๔ ต้องมีการตรวจสอบ และทดสอบระบบ รวมถึงอุปกรณ์สนับสนุนอย่างสม่ำเสมอเพื่อให้มั่นใจว่าอุปกรณ์ดังกล่าวยังสามารถทำงานได้อย่างเหมาะสม

๒๔.๑๑.๕ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (Cabling Security) ต้องได้รับการติดตั้งด้วยวิธีการที่เป็นมาตรฐานและสามารถป้องกันภัยคุกคามที่อาจเกิดกับสายไฟฟ้าและสายสื่อสารได้

(๑) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่าง ๆ กัดสาย

/(๒) ให้เดินสาย ...

(๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๔) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒๔.๑๑.๖ ต้องมีการติดป้ายและระบุรายละเอียดของสายและเต้ารับอย่างชัดเจน เพื่อให้สามารถบริหารจัดการและแก้ไขปัญหาได้อย่างสะดวก

๒๔.๑๑.๗ ต้องมีการบำรุงรักษาอุปกรณ์ (Equipment Maintenance) อย่างเหมาะสม

(๑) กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมสอดส่องดูแลการปฏิบัติงานของผู้รับเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน สศค.

(๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๔.๑๑.๘ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอก สศค. (Security of Equipment Off - Premises)

กำหนดมาตรการรักษาความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของ สศค. ออกไปใช้งานข้างนอก (Removal of Property)

(๑) ต้องทำการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอก สศค.

(๒) บันทึกข้อมูลการนำอุปกรณ์ออกนอก สศค. เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๓) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของ สศค. ไว้ในที่สาธารณะ

(๔) รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

/(๕) กรณีที่จำเป็นต้อง ...

(๕) กรณีที่จำเป็นต้องส่งอุปกรณ์ที่มีข้อมูลอยู่ออกไปดำเนินการซ่อมแซมหรือบำรุงรักษานอกพื้นที่ ต้องทำการสำรอง ทำลายข้อมูล ลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม รวมถึงซอฟต์แวร์ด้วยวิธีการที่ไม่สามารถกู้คืนข้อมูลได้ก่อนส่งออกทุกครั้ง กรณีที่ไม่สามารถทำลายข้อมูลได้เนื่องจากปัญหาด้านเทคนิค กำหนดให้เจ้าของอุปกรณ์และเจ้าของข้อมูลร่วมกันพิจารณาหาวิธีการที่เหมาะสมโดยคำนึงถึงความเสี่ยงที่ข้อมูลจะรั่วไหลเป็นหลัก

๒๔.๑๑.๙ การทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะทำลายอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๒๔.๑๑.๑๐ ผู้ดูแลระบบต้องปฏิบัติตามเงื่อนไขในการรับประกันอุปกรณ์อย่างเคร่งครัด

๒๔.๑๑.๑๑ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีการสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของ สศค. ที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ได้แก่ ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศ และควบคุมความชื้น เป็นต้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากความล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๒๕. นโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของ สศค. และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งสามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของ สศค. ได้อย่างถูกต้อง ด้วยการกำหนดรายละเอียดที่เกี่ยวกับการกำหนดระดับสิทธิ์ การควบคุมและจำกัดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

/ที่เหมาะสม ...

และระบบเครือข่ายที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงการมอบหมายสิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง โดยมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๒๕.๑ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

กำหนดวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย โดยมีแนวปฏิบัติการเข้าถึงและการใช้งานสารสนเทศที่เหมาะสม ดังนี้

๒๕.๑.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

(๑) การลงทะเบียนผู้ใช้งานทั่วไป สำหรับระบบสารสนเทศที่จำเป็นพื้นฐานซึ่งเป็นการเข้าใช้งานบนระบบอินทราเน็ต (Intranet) ได้แก่ ระบบการลงเวลาการปฏิบัติงาน ระบบการลาอิเล็กทรอนิกส์ ระบบจองรถยนต์ ระบบการจองห้องประชุม ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ ระบบ e-Learning เป็นต้น รวมถึงการเข้าใช้งานบนระบบอินเทอร์เน็ต (Internet) ได้แก่ ระบบเว็บไซต์ของ สศค. ระบบไปรษณีย์อิเล็กทรอนิกส์ (e-mail) เป็นต้น ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบ จะประสานกับส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม เพื่อดำเนินการลงทะเบียนผู้ใช้งานทั่วไป รวมถึงการตัดออกจากทะเบียนผู้ใช้งานทั่วไป

(๒) การลงทะเบียนผู้ใช้งานระบบสารสนเทศด้านการอำนวยการ ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ ระบบบริหารจัดการวัสดุและครุภัณฑ์ ระบบการขอจัดซื้อจัดจ้าง ระบบบริหารจัดการงบประมาณ เป็นต้น ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะประสานกับส่วนบริหารทั่วไป ส่วนบริหารงานพัสดุ และส่วนบริหารงานคลัง สำนักงานเลขานุการกรม เพื่อดำเนินการลงทะเบียนผู้ใช้งานระบบ

(๓) การลงทะเบียนผู้ใช้งานระบบสารสนเทศสนับสนุนภารกิจหลัก ได้แก่ ระบบสารสนเทศสถาบันการเงิน (FIs Management System: FI) ระบบสารสนเทศสถาบันการเงินเฉพาะกิจ (SFIs Management System: SFI) ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะประสานกับหน่วยงานภายใน (กอง/กลุ่ม/ศูนย์) ที่เป็นเจ้าของระบบงาน เพื่อดำเนินการลงทะเบียนผู้ใช้งานระบบตามสิทธิ์การเข้าใช้ระบบอย่างถูกต้อง เพียงพอ และเหมาะสมตามความจำเป็นในการใช้งาน ทั้งนี้ ภายหลังจากที่ได้รับแจ้งรายชื่อ ตำแหน่งและวัตถุประสงค์ในการใช้ระบบงาน โดย กอง/กลุ่ม/ศูนย์ ต้องจัดทำเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบเป็นลายลักษณ์อักษรส่งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศอนุมัติ และเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

/(๔) ผู้ดูแลระบบ ...

(๔) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และการกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นบันทึกและกรอกแบบฟอร์มที่ศูนย์เทคโนโลยีสารสนเทศกำหนด เพื่อขอสิทธิ์ในการเข้าระบบเฉพาะส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้อำนวยการกอง/กลุ่ม/ศูนย์ เพื่อการจัดเก็บไว้เป็นหลักฐาน

(๕) หากบุคลากรมีการโอน/ย้าย/ลาออก/สิ้นสุดการจ้าง หรือเมื่อเปลี่ยนตำแหน่งงานภายใน สศค. หรือกรณีไปช่วยราชการที่อื่น ศูนย์เทคโนโลยีสารสนเทศจะประสานกับส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม เพื่อทำการระงับการใช้งานของรหัสผ่านทันทีเมื่อบุคลากรพ้นจากภารกิจ รวมถึงทำการยกเลิกและตัดสิทธิ์การเข้าใช้งานระบบสารสนเทศทุกระบบพร้อมลบชื่อออกจากทะเบียนผู้ใช้งานทั่วไปและผู้ใช้งานระบบภายใน ๓๐ วัน ทั้งนี้ ภายหลังจากที่ได้รับแจ้งรายชื่อ ตำแหน่งและวันที่มีผลบังคับใช้ โดยมีหลักฐานเป็นลายลักษณ์อักษรจากส่วนบริหารทรัพยากรบุคคล สำนักงานเลขานุการกรม หรือหน่วยงานที่เกี่ยวข้องแล้ว

(๖) ศูนย์เทคโนโลยีสารสนเทศจะกำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในเบื้องต้น โดยใช้ข้อมูลจากส่วนกลางที่จัดเก็บใน Active Directory (AD) และส่งมอบให้แก่ผู้ใช้งานซึ่งระบบงานอนุญาตให้ผู้ใช้งานเปลี่ยนรหัสผ่านได้ด้วยตนเอง และหากมีปัญหา ได้แก่ ผู้ใช้งานลืมรหัสผ่าน เป็นต้น ศูนย์เทคโนโลยีสารสนเทศจะเป็นผู้ดำเนินการกำหนดรหัสผ่านใหม่ให้หลังจากได้รับการแจ้งจากผู้ใช้งาน

๒๕.๑.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

ศูนย์เทคโนโลยีสารสนเทศซึ่งเป็นผู้ดูแลบริหารจัดการระบบ (System Administrator) มีหน้าที่บริหารจัดการสิทธิ์ของผู้ใช้งาน ควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศ

(๑) กำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบตัวตนจริงและควบคุมการเข้าถึงข้อมูลในแต่ละชั้นความลับ โดยจำแนกผู้ใช้งานออกเป็นกลุ่มต่าง ๆ ตามระดับการใช้งานที่เหมาะสม โดยคำนึงถึงชั้นความลับของข้อมูลเพื่อกำหนดกลุ่มผู้ใช้งานและระดับการใช้ข้อมูลในการปฏิบัติงาน ได้แก่ กลุ่มผู้ใช้ที่มีสิทธิ์เข้าถึงระบบฐานข้อมูลและแฟ้มข้อมูล (Database and File System) กลุ่มผู้ใช้ที่มีสิทธิ์เข้าถึงเฉพาะข้อมูลสารสนเทศ รวมถึงผู้ใช้ระดับใดควรมีสิทธิ์แก้ไขข้อมูล ระดับใดควรสร้าง/ลบข้อมูลได้ และระดับใดสามารถเรียกดูข้อมูลได้เพียงอย่างเดียว เป็นต้น

/(๒) กำหนด ...

(๒) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ โดยการกำหนดสิทธิ์ต่าง ๆ ให้แก่ผู้ใช้งานในแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ สิทธิ์ในการอ่านอย่างเดียว สิทธิ์ในการสร้างข้อมูล สิทธิ์ในการป้อนข้อมูล สิทธิ์ในการแก้ไข สิทธิ์ในการอนุมัติ รวมถึงการไม่มีสิทธิ์ โดยผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของ สศค. จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๓) กำหนดสิทธิ์และมอบอำนาจการใช้งานสารสนเทศแต่ละชนิดเพื่อควบคุมการอนุญาตให้เข้าถึงสารสนเทศที่สำคัญ ควรแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนงานคอมพิวเตอร์ ตามแนวปฏิบัติที่ดี (Best Practice) ดังนี้

- มีหน่วยงานควบคุมการให้สิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด
- แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์
- กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติอยู่ในศูนย์เทคโนโลยีสารสนเทศอย่างชัดเจนเป็นลายลักษณ์อักษร
- มีบุคลากรสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น ได้แก่ ผู้บริหารระบบเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เป็นต้น
- ให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้อำนวยการกอง/กลุ่ม/ศูนย์ เป็นลายลักษณ์อักษร
- มีการตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที
- จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอสำหรับระบบสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail) ระบบอินเทอร์เน็ต ระบบอินทราเน็ต

(๔) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุดนอกเหนือจากผู้ใช้งานปกติ ได้แก่ ผู้ตรวจสอบภายใน เป็นต้น ต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา เลขานุการกรม หรือผู้อำนวยการกอง/กลุ่ม/ศูนย์ นั้น ๆ ก่อน และต้องควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ

/ควบคุม ...

- ควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน เป็นต้น

(๕) หน่วยงานภายในที่เกี่ยวข้องในการจัดทำข้อมูล (เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน) จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามภารกิจและการปฏิบัติงานในหน้าที่เท่านั้น เนื่องจากการใช้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(๖) ผู้ดูแลระบบร่วมกับหน่วยงานภายในที่เกี่ยวข้องในการจัดทำข้อมูล (เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน) จะต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติเกี่ยวกับข้อมูล สารสนเทศ และ/หรือระบบงานที่รับผิดชอบ เพื่อให้ผู้ใช้งานสามารถนำข้อมูลไปใช้ หรือใช้ระบบงานได้อย่างถูกต้อง มีประสิทธิภาพ และเป็นมาตรฐานเดียวกัน

(๗) ผู้ดูแลระบบร่วมกับหน่วยงานภายในที่เกี่ยวข้องในการจัดทำข้อมูล (เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน) ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล กำหนดประเภทข้อมูล และควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๘) ระบบงานสารสนเทศต้องออกแบบให้มีระบบการตรวจสอบ โดยต้องมีการเก็บบันทึก (Record) เป็นหลักฐานที่สามารถทำการติดตามตรวจสอบ (Audit Trial) ภายหลังได้ว่า ณ เวลาที่เข้าถึงระบบของผู้ใช้ (Events Logging) ว่าผู้ใช้เป็นใคร เข้าระบบทำอะไร จากที่ไหน และทำสำเร็จหรือไม่ โดยที่แฟ้มข้อมูลของระบบการตรวจสอบจะต้องได้รับการปกป้องและตรวจสอบได้เสมอ

(๙) ระบบฐานข้อมูลที่สำคัญ ได้แก่ ระบบสารสนเทศที่เกี่ยวข้องกับการเงิน เป็นต้น ต้องสามารถบันทึกรายละเอียดเกี่ยวกับการเข้าถึงฐานข้อมูลในแต่ละครั้ง และต้องมีรายละเอียดที่เพียงพอเพื่อประโยชน์ในการอ้างอิงได้ภายหลัง ได้แก่ วัน เวลาที่เข้าถึง ชื่อเจ้าหน้าที่ที่เข้าถึง และวัตถุประสงค์ของการเข้าถึง เป็นต้น

(๑๐) ต้องจัดให้มีการติดตั้งระบบบันทึก ติดตามการใช้งาน และตรวจสอบการละเมิดความปลอดภัยของระบบเทคโนโลยีสารสนเทศของ สศค.

/(๑๑) ต้องจัด ...

(๑๑) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า – ออกสถานที่ตั้งของระบบ ทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

(๑๒) ต้องมีการจำกัดและควบคุมการเข้าถึง Source Code ของโปรแกรมเพื่อหลีกเลี่ยงการเปลี่ยนแปลงโดยไม่เจตนา

๒๕.๑.๓ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

ผู้ดูแลระบบร่วมกับหน่วยงานภายในที่เกี่ยวข้องในการจัดทำข้อมูล (เจ้าของข้อมูลและ/หรือ เจ้าของระบบงาน) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๑) ทบทวนสิทธิ์การเข้าใช้งานและสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานและปรับปรุงบัญชีผู้ใช้งานให้มีความเหมาะสมอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด ทุก ๆ ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับเปลี่ยนเคลื่อนย้ายบุคลากร เช่น การโอน/ย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ ลาออก สิ้นสุด/ยกเลิกการจ้าง เป็นต้น เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๒) การให้อำนาจสำหรับสิทธิ์การเข้าถึงพิเศษ ต้องทบทวนบ่อยกว่าปกติ ทุก ๆ ๓ เดือน

(๓) การจัดสรรสิทธิ์พิเศษ ต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดเพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิ์พิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

(๔) การเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิ์พิเศษต้องถูกบันทึกเพื่อการทบทวน

(๕) กรณีมีปัญหาการใช้หรือนำระบบงานไปปฏิบัติโดยไม่ได้รับอนุญาต ศูนย์เทคโนโลยีสารสนเทศจะดำเนินการติดตาม ตรวจสอบ และทบทวนการใช้งาน หากมีผลที่คาดว่าจะกระทบถึงระบบงานในอนาคต ศูนย์เทคโนโลยีสารสนเทศสงวนสิทธิ์พิจารณายกเลิกการใช้งานนั้น

๒๕.๒ การบริหารจัดการการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒๕.๒.๑ ผู้ดูแลระบบต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานสำหรับการลงทะเบียนบุคลากรใหม่ของ สศค. รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การโอน/ย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ ลาออก สิ้นสุด/ยกเลิกการจ้าง เป็นต้น

/๒๕.๒.๒ ผู้ดูแล ...

๒๕.๒.๒ ผู้ดูแลระบบต้องกำหนดวิธีการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒๕.๒.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบมีการโอน/ย้ายหน่วยงาน เลื่อนตำแหน่ง เปลี่ยนหน้าที่รับผิดชอบ ลาออก สิ้นสุด/ยกเลิกการจ้าง เป็นต้น

(๒) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๓) ควรกำหนดให้ผู้ใช้งานตอบกลับหลังจากได้รับรหัสผ่าน

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) ควรกำหนดให้ชื่อผู้ใช้และรหัสผ่านต้องไม่ซ้ำกัน

(๕) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง รวมถึงควรมีการกำหนดสิทธิ์พิเศษที่ได้รับนั้นว่าสามารถเข้าถึงได้จนถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานนั้นต่างจากรหัสผู้ใช้งานตามปกติ

๒๕.๒.๔ กรณีที่จำเป็นต้องใช้สิทธิ์พิเศษในการบริหารจัดการระบบ ผู้ใช้งานหรือผู้ร้องขอต้องบันทึกเหตุผลความจำเป็นและระบุรายละเอียดการใช้งานสิทธิ์พิเศษในการบริหารจัดการระบบทุกครั้ง

๒๕.๒.๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภท ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

/(๓) ควรกำหนด ...

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) ควรกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของ สศค. เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนจัดส่ง เป็นต้น

๒๕.๓ การควบคุมการเข้าถึงระบบเครือข่าย

๒๕.๓.๑ ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน หรือวิธีการทางเทคนิคอื่น ๆ ที่เหมาะสมและปลอดภัย

๒๕.๓.๒ ผู้ดูแลระบบต้องกำหนดให้มีวิธีจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

๒๕.๓.๓ ระบบเครือข่ายทั้งหมดของ สศค. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สศค. ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๒๕.๓.๔ ต้องมีการติดตั้ง Firewall เพื่อป้องกันการบุกรุก การเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาตจากบุคคลภายนอกหรือผู้ไม่ประสงค์ดี

๒๕.๓.๕ การเข้าสู่ระบบเครือข่ายภายใน สศค. โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๒๕.๓.๖ เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของ สศค. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๒๕.๓.๗ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒๕.๓.๘ การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

/๒๕.๓.๙ ผู้ดูแล ...

๒๕.๓.๙ ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย รวมถึงกำหนดการแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๒๕.๔ การเข้ารหัสข้อมูล (Cryptography)

๒๕.๔.๑ ต้องกำหนดวิธีการและผู้รับผิดชอบในการบริหารจัดการกุญแจ ดังนี้

(๑) การสร้างกุญแจรหัส (Key Generation) กุญแจรหัสต้องเป็นรหัสผ่านที่มีคุณภาพและยากต่อการคาดเดา

(๒) การแจกจ่ายกุญแจรหัส (Key Distribution) กุญแจรหัส หรือรหัสผ่านเป็นข้อมูลที่มีความสำคัญ ดังนั้นการจัดส่งต้องกระทำอย่างระมัดระวังความปลอดภัย และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๓) การสำรองกุญแจรหัส (Key Storage) กุญแจรหัสที่ใช้งานอยู่ต้องจัดเก็บแยกกับข้อมูลที่เข้ารหัสไว้

(๔) การเพิกถอนกุญแจรหัส (Key Revoking) ต้องทำการเพิกถอนกุญแจรหัสเมื่อเกิดปัญหากุญแจรหัสสูญหาย หรือชำรุดไม่สามารถใช้งานได้

๒๕.๕ พิจารณาใช้เทคนิคสำหรับการปิดบังข้อมูล (Data masking) เพื่อป้องกันไม่ให้ข้อมูลดังกล่าวถูกมองเห็น หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต โดยข้อมูลนั้นอาจเป็นข้อมูลที่อยู่ในฟิลด์ต่าง ๆ ของฐานข้อมูลที่มีความสำคัญ ข้อมูลในระบบซึ่งอาจเป็นข้อมูลส่วนบุคคล ข้อมูลลับ หรือข้อมูลที่อ่อนไหว โดยเทคนิคที่ใช้ควรคำนึงถึงความเหมาะสมและข้อจำกัดของระบบ

๒๕.๖ แนวทางการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

ศูนย์เทคโนโลยีสารสนเทศเป็นผู้บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุมและมีความมั่นคงปลอดภัย เนื่องจากรหัสผ่านเป็นวิธีพื้นฐานในการตรวจสอบตัวตนของผู้ใช้ระบบ ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่า ผู้ที่เข้ามาใช้ระบบนั้น คือบุคคลที่มีสิทธิ์เข้าสู่ระบบของ สศค. อย่างแท้จริง กำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านดังนี้

๒๕.๖.๑ ผู้ใช้ระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนแก่บุคคลอื่น

๒๕.๖.๒ ผู้ใช้รายใหม่จะได้รับรหัสผ่านเริ่มแรก (รหัสผ่านชั่วคราว) ในการใช้ผ่านเข้าสู่ระบบในครั้งแรก และระบบต้องบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านโดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก ผู้ใช้สามารถสร้างรหัสผ่านที่มีคุณภาพและยากต่อการคาดเดาตามแนวปฏิบัติที่ดีในการใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)

/๒๒.๖.๓ ไม่เก็บรหัส ...

๒๕.๖.๓ ไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้

๒๕.๖.๔ รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้ที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้ที่มีสิทธิ์ใช้งานระบบได้ ได้แก่ มีรายชื่อในระบบ Active Directory (AD) เป็นต้น

๒๕.๖.๕ แสดงรหัสผ่านในรูปของสัญลักษณ์ หรือตัวอักษร “x” หรือ “o” หรือ “•” ในขณะพิมพ์รหัสผ่านแต่ละตัวอักษร โดยต้องไม่ปรากฏหรือแสดงรหัสผ่านที่แท้จริงออกมา

๒๕.๖.๖ การตั้งรหัสผ่าน ควรหลีกเลี่ยงการใช้ข้อมูลที่เกี่ยวข้องกับ สศค. ข้อมูลส่วนตัว ได้แก่ ชื่อ นามสกุล นามแฝง วันเดือนปีเกิด ที่อยู่ ทะเบียนยานพาหนะ หมายเลขโทรศัพท์ เลขที่บัตรประชาชน เลขที่บัตรประกันสังคม รหัสบัตรต่าง ๆ ชื่อบุคคลในครอบครัว เป็นต้น รวมถึงต้องไม่ใช้ชื่อภาพยนตร์ ชื่อสถานที่หรือชื่อสิ่งลึกลับ ศัพท์ที่มาจากพจนานุกรม เนื่องจากข้อมูลต่าง ๆ เหล่านี้ ง่ายต่อการคาดเดาของผู้โจมตีระบบ (Hackers)

๒๕.๖.๗ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Saved Password) สำหรับเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองอยู่ รวมถึงไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

๒๕.๖.๘ ควรกำหนดวิธีการส่งมอบรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย ได้แก่ ใส่ซองปิดผนึก การส่งทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail) และบังคับให้ใส่วัน เดือน ปีเกิด ในการเปิดอ่านไปรษณีย์อิเล็กทรอนิกส์ และผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน กรณีระบบที่ต้องการความมั่นคงปลอดภัยมากเป็นพิเศษ กำหนดให้การจัดส่งและการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัยมากยิ่งขึ้น โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน พร้อมแนบเอกสาร “แนวปฏิบัติที่ดีในการใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๒๕.๖.๙ การตั้งรหัสผ่าน ควรมีส่วนประกอบของอักษร อักขระพิเศษ และ/หรือ ตัวเลขที่ประสมกันตามลักษณะดังต่อไปนี้

- ความยาวอย่างน้อย ๘ ตัวอักษรหรือตามที่ผู้บริหารจัดการระบบกำหนด
- อักษรตัวพิมพ์ใหญ่ ได้แก่ A, B, C, ... เป็นต้น
- อักษรตัวพิมพ์เล็ก ได้แก่ a, b, c, ... เป็นต้น
- ตัวเลข ได้แก่ ๐, ๑, ๒, ... เป็นต้น
- สัญลักษณ์พิเศษ ได้แก่ !, @, #, $, ... เป็นต้น

๒๕.๖.๑๐ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๒๕.๖.๑๑ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

/๒๕.๖.๑๒ รหัสผ่าน ...

๒๕.๖.๑๒ รหัสผ่านเข้าระบบบริหารจัดการด้านเครือข่ายและระบบงานที่สำคัญ ได้แก่ การเข้า Root, Enable, NT Admin, Application Admin Account เป็นต้น จะต้องมีการเปลี่ยนรหัสผ่านเป็นประจำอย่างน้อยทุก ๓ เดือน

๒๕.๖.๑๔ รหัสผ่านของผู้ใช้งาน ได้แก่ e-mail, Website, Desktop Computer, Notebook และระบบเทคโนโลยีสารสนเทศ เป็นต้น ต้องเปลี่ยนเป็นประจำอย่างน้อยทุก ๖ เดือน ทั้งนี้แนะนำให้เปลี่ยนเป็นประจำทุก ๓ เดือน จะสร้างความปลอดภัยได้ดียิ่งขึ้น

๒๕.๖.๑๕ ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน ถ้ารหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๒๕.๖.๑๖ ผู้ใช้งานไม่ควรเปลี่ยนรหัสผ่านของผู้อื่น ยกเว้นผู้มีหน้าที่ในการบริหารจัดการรายชื่อผู้ใช้งานและรหัสผ่านเท่านั้น

๒๕.๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของ สศค. เพื่อควบคุมและจำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบปฏิบัติการได้ โดยกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งานที่ได้รับมอบหมายให้เข้าใช้ งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของ สศค. และแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๒๕.๗.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

(๑) ต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ทุกครั้งที่เข้าใช้งานระบบ

(๒) ต้องกำหนดรหัสผ่านที่มีคุณภาพดี (Good Password)

(๓) ต้องทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเครื่องคอมพิวเตอร์ หรือไม่อยู่ที่หน้าจอ

(๔) ต้องทำการ Logout ออกจากระบบปฏิบัติการทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒๕.๗.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม

(๑) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username)

/(๒) การพิสูจน์ ...

(๒) การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) โดยระบบมีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Smart Card ร่วมได้

๒๕.๗.๓ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๑) มีระบบบริหารจัดการรหัสผ่านซึ่งจะติดตั้งบนระบบเครือข่ายสารสนเทศของ สศค. โดยระบบจะยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

(๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ โดยปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ที่ได้กำหนดไว้

(๓) มีระบบแจ้งระดับความความปลอดภัยของรหัสผ่าน

๒๕.๗.๔ ควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utilities Program/Software) เพื่อป้องกันการละเมิดลิขสิทธิ์หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว เนื่องจากการใช้งานซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกหรือโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ซึ่งอาจก่อให้เกิดความเสี่ยงในการใช้งานโปรแกรมไม่ประสงค์ดี จึงต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์

(๑) จำกัดสิทธิ์การเข้าถึงและกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก หากไม่ได้ใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ห้ามติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก สศค. ที่ไม่มีลิขสิทธิ์ รวมทั้งการใช้ไฟล์อื่น ๆ ที่ไม่อนุญาตให้ใช้งาน

(๗) ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

/ (๘) ให้ติดตั้ง ...

(๘) ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศ

(๙) กำหนดหน้าที่ความรับผิดชอบ ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่ตรวจพบ

(๑๐) ติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

(๑๑) สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๒๕.๗.๕ การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน (Session Time - out)

(๑) กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาทีเป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที หรือตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่าย มีการยกเลิกและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

(๓) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง โดยเฉพาะระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๔) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๕) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๒๕.๗.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

/เพื่อให้ ...

เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของ สศค. ตามปกติเท่านั้น และกำหนดให้ระบบยกเลิกการเชื่อมต่อหากผู้ใช้งานไม่มีการใช้งานเกิน ๓๐ นาที

(๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ หรือระบบงานที่มีความสำคัญสูง หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอก สศค.) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

(๓) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๒๖. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy)

<u>วัตถุประสงค์</u>

เพื่อให้ผู้ใช้บริการได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามเพื่อเป็นการป้องกันทรัพยากรและข้อมูลของ สศค. ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ โดยศูนย์เทคโนโลยีสารสนเทศในฐานะผู้ดูแลระบบเครือข่ายของ สศค. ดำเนินการตามแนวทางดังต่อไปนี้

๒๖.๑ ต้องจัดทำเอกสารคู่มือ ขั้นตอนปฏิบัติหรือสิ่งอื่นใดที่จำเป็นต่อการบริหารจัดการระบบสารสนเทศเป็นลายลักษณ์อักษร และจัดเก็บไว้อย่างเหมาะสมและสะดวกต่อการนำมาใช้งาน

๒๖.๒ การแบ่งแยกเครือข่าย (Segregation In Networks)

มีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศเพื่ออำนวยความสะดวกในการควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ ได้แก่ เครือข่ายภายนอก (External Zone) เครือข่ายสาธารณะ (Public Zone) เครือข่ายภายใน สศค. (Internal Zone) และเครือข่ายไร้สาย (Wireless)

๒๖.๓ ต้องควบคุมการเข้าถึงระบบเครือข่ายอย่างเหมาะสมเพื่อให้การบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพให้สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy)

๒๖.๔ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

กำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้บริหารจัดการสิทธิ์ให้แก่ผู้ใช้งานในการเข้าถึงระบบเครือข่ายและทรัพยากรเครือข่ายเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

/๒๖.๔.๑ ผู้ใช้งาน ...

๒๖.๔.๑ ผู้ใช้งานมีสิทธิ์ในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตตามภารกิจหน้าที่ของตนเองเท่านั้น

๒๖.๔.๒ กำหนดหมายเลขเครือข่าย (IP Address) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อแสดงตัวตนและควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบเครือข่ายทุกครั้ง และห้ามมิให้เปิดเผยหมายเลขเครือข่าย (IP Address) แก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้องกับการใช้หมายเลขเครือข่ายดังกล่าว

๒๖.๔.๓ กำหนดผู้รับผิดชอบในการกำหนด หรือแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งผู้ดูแลระบบเครือข่ายให้รับทราบทุกครั้ง

๒๖.๔.๔ มีการบริหารจัดการระบบเครือข่ายโดยการแปลงหมายเลขเครือข่ายเพื่อแบ่งแยกเครือข่ายย่อยเพื่อจำกัดสิทธิ์ในการใช้งานระบบเครือข่ายร่วมกันภายใน สศค. (กอง/กลุ่ม/ศูนย์) ที่มีภารกิจหน้าที่เดียวกัน ได้แก่ การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่าย เป็นต้น

๒๖.๔.๕ ระบบเครือข่ายที่มีความจำเป็นต้องเชื่อมต่อไปยังเครือข่ายภายนอก สศค. จะต้องทำการเชื่อมต่อกับอุปกรณ์รักษาความปลอดภัย (Firewall) และติดตั้งระบบป้องกันการรุกราน (Intrusion Prevention System : IPS)

๒๖.๕ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) โดยการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

๒๖.๕.๑ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification In Networks) มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง

(๑) กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

/(๒) มีการควบคุม ...

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๑.๑) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๑.๒) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับอนุมัติจาก สศค. และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๑.๓) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศเท่านั้น ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายมาติดตั้งโดยมิได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๑.๔) กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก โดยบันทึกการเข้า/ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

(๑.๕) มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (เก็บ Log) ของอุปกรณ์เครือข่ายเพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

๒๖.๕.๒ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

(๑) ระบบเครือข่ายทั้งหมดของ สศค. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สศค. ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือ Hardware อื่น ๆ เป็นต้น

(๒) กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy, Firewall, และ IPS/IDS เป็นต้น

(๓) การควบคุมการเข้าถึงระบบเครือข่ายภายในของ สศค.

(๓.๑) การเข้าสู่ระบบเครือข่ายภายในของ สศค. โดยผ่านทางระบบอินเทอร์เน็ตต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมายก่อนทุกครั้ง

(๓.๒) การเข้าสู่ระบบเครือข่ายภายใน สศค. ผ่านทางระบบอินเทอร์เน็ตต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

/(๔) ควบคุม ...

(๔) ควบคุมการเข้าใช้งานระบบเครือข่ายจากภายนอก (Remote Access)

(๔.๑) ต้องมีการควบคุมอย่างเข้มงวด โดยใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน และต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของ สศค. มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(๔.๒) บังคับใช้เส้นทางเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อจำกัดการใช้เส้นทางบนเครือข่ายโดยทำการเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้

(๔.๓) การอนุญาตให้ผู้ใช้งานหรือผู้ให้บริการภายนอกเข้าสู่ระบบเครือข่ายจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น หากมีความจำเป็นต้องเข้าถึงข้อมูลโดยเข้าสู่ระบบเครือข่ายจากระยะไกลด้วยวิธีการใด ๆ จะต้องขอสิทธิ์ในการเข้าสู่ระบบเครือข่ายจากระยะไกลพร้อมระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ สศค. อย่างเพียงพอและต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมายก่อนทุกครั้ง และต้องแสดงหลักฐานการได้รับอนุญาตให้เข้าสู่ระบบจากระยะไกลต่อผู้บริหารสิทธิ์

(๔.๔) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ โดยกำหนดบุคลากรผู้มีหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล และต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

(๔.๕) ต้องมีการควบคุมสิทธิ์การใช้งานและการเข้าถึงข้อมูลสารสนเทศอย่างเหมาะสมด้วยวิธีการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก สศค. (User Authentication for External Connections)

(๔.๕.๑) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username) และพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน

(๔.๕.๒) การเข้าสู่ระบบสารสนเทศของ สศค. จากระบบอินเทอร์เน็ตนั้นต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมาย

/(๔.๕ ๓) การใช้งาน ...

(๔.๕ ๓) การใช้งานระบบอินเทอร์เน็ตเพื่อเข้ามายังระบบสารสนเทศของ สศค. ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN เป็นต้น

(๔.๕.๔) กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะหรือเครือข่ายระบบอินเทอร์เน็ต หรือเครือข่ายไร้สาย

(๔.๕.๕) กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

(๔.๕.๖) กำหนดมาตรการเพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารเทศต่าง ๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

(๔.๖) มีการควบคุมช่องทาง (Port) ที่ใช้เชื่อมต่อเข้าสู่ระบบเครือข่ายอย่างรัดกุม ไม่เปิด Port ทิ้งไว้โดยไม่จำเป็น และให้ตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

(๔.๗) การเชื่อมต่อระยะไกลกับบริการที่สำคัญของ สศค.

- ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกลเมื่อมีความจำเป็นเท่านั้น
- ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
- ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของ สศค. เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการในการปฏิบัติงาน
- จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

(๔.๘) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic And Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

/(๔.๘.๑) มีการติดตั้ง ...

(๔.๘.๑) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของ สศค. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง

(๔.๘.๒) IP Address ของระบบงานเครือข่ายภายใน สศค. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศได้โดยง่าย

(๔.๘.๓) หากผู้ดูแลบริหารจัดการระบบ (Administrator) จำเป็นต้องใช้งานผ่านพอร์ตจะต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

(๔.๘.๔) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๔.๘.๕) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๔.๘.๖) ปิดการใช้งานเพื่อป้องกันพอร์ตที่ไม่มีการใช้งาน

(๔.๘.๗) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๒๖.๖ ควบคุมการดำเนินการเปลี่ยนแปลงต่าง ๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยต่ออุปกรณ์ประมวลผลสารสนเทศและระบบสารสนเทศ โดยที่ผู้ดูแลระบบต้องปฏิบัติตามนโยบายด้านการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management Policy & Procedure) ทั้งนี้การเปลี่ยนแปลงต่ออุปกรณ์ ซอฟต์แวร์ และขั้นตอนการปฏิบัติงานในระบบเทคโนโลยีสารสนเทศต้องได้รับการควบคุมอย่างเหมาะสม

๒๖.๗ ติดตามและเฝ้าระวังการใช้ทรัพยากรของระบบเพื่อใช้ปรับปรุงและคาดการณ์ความต้องการทางด้านทรัพยากรของระบบที่อาจจำเป็นต้องเพิ่มเติมขีดความสามารถหรือลดความต้องการด้านทรัพยากรของระบบ เพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ

๒๖.๘ พิจารณาแยกสภาพแวดล้อมของระบบที่มีการพัฒนาหรือทดสอบออกจากระบบที่ให้บริการจริง เพื่อลดความเสี่ยงในการเข้าถึงการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต หรือความล้มเหลวของการให้บริการ

/๒๖.๙ นาฬิกา ...

๒๖.๙ นาฬิกาของอุปกรณ์ประมวลผลสารสนเทศและระบบสารสนเทศ ต้องมีการตั้งให้ตรงและถูกต้องโดยเทียบกับแหล่งอ้างอิงเวลาที่มีความน่าเชื่อถือ เช่น สถาบันมาตรวิทยา กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)

๒๖.๑๐ ซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นที่จะสามารถติดตั้งในระบบปฏิบัติการได้เพื่อลดความเสี่ยงที่จะทำให้ระบบที่ให้บริการเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

๒๖.๑๑ ติดตามข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานอย่างสม่ำเสมอและมีการบริหารจัดการเพื่อแก้ไขช่องโหว่ดังกล่าว โดยการประเมินความเสี่ยงของช่องโหว่ดังกล่าวและกำหนดมาตรการที่เหมาะสมเพื่อจัดการกับความเสี่ยงอันเกิดจากช่องโหว่ทางเทคนิคของระบบสารสนเทศและปฏิบัติตามนโยบายการบริหารจัดการช่องโหว่ (Vulnerability Management Policy)

๒๖.๑๒ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อให้มีการตอบสนองได้อย่างรวดเร็ว มีประสิทธิภาพ และตอบสนองเหตุการณ์ดังกล่าวตามลำดับ

๒๖.๑๓ กำหนดช่องทางสำหรับใช้ในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

๒๖.๑๔ ภายหลังการรับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยแล้ว ต้องประเมินสถานการณ์ดังกล่าวเพื่อตัดสินใจว่าสถานการณ์นั้นเป็นเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือไม่ ซึ่งผลการประเมินและการตัดสินใจนั้นจำเป็นต้องถูกบันทึกรายละเอียดไว้เพื่อใช้อ้างอิงและทวนสอบต่อไปในอนาคต

๒๖.๑๕ ต้องมีการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย

๒๖.๑๖ ต้องรวบรวม จัดหาและจัดเก็บข้อมูลสารสนเทศเพื่อใช้เป็นหลักฐาน

๒๖.๑๗ ต้องมีการเก็บรวบรวมข้อมูลความรู้ที่ได้รับจากการวิเคราะห์และแก้ปัญหาของเหตุการณ์ด้านความมั่นคงปลอดภัยที่เคยเกิดขึ้นเพื่อนำมาใช้ลดโอกาสที่อาจเกิดขึ้นในอนาคต

๒๖.๑๘ ต้องจัดเตรียมอุปกรณ์ประมวลผลสำรองให้เพียงพอ และมีความพร้อมใช้ โดยกำหนดให้มีการทดสอบอุปกรณ์ประมวลผลสำรอง เพื่อให้มั่นใจว่าเมื่อระบบล้มเหลวแล้วอุปกรณ์ประมวลผลสำรองยังสามารถใช้งานได้

๒๗. นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

/๒๗.๑ การติดตั้ง ...

๒๗.๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ

๒๗.๒ กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๒๗.๒.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริง ๆ ต้องวางในระบบเครือข่ายภายในที่เป็น Internal Network ต้องมีการพิสูจน์ยืนยันตัวตนและการเข้ารหัส (Authentication, Encryption)

๒๗.๒.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น

๒๗.๒.๓ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย โดยกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๒๗.๒.๔ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๒๗.๒.๕ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๒๗.๒.๖ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

๒๗.๒.๗ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของ สศค.

๒๗.๒.๘ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่อาจเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน กรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบทันที

/๒๘. นโยบาย ...

๒๘. นโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมความมั่นคงปลอดภัยของไฟร์วอลล์ โดยการกำหนดค่าต่าง ๆ ให้เหมาะสมตามความต้องการในการปฏิบัติงาน รวมทั้งมีการทบทวนการกำหนดค่าอย่างสม่ำเสมอ ทั้งนี้ ผู้ที่ควบคุมดูแลต้องเป็นผู้ดูแลระบบที่มีสิทธิ์ในการเข้าถึงการตั้งค่าของไฟร์วอลล์ตามนโยบายเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน สศค.

๒๘.๑ ศูนย์เทคโนโลยีสารสนเทศมีหน้าที่ในการบริหารจัดการ ติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมดของ สศค.

๒๘.๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๒๘.๓ ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่ได้รับอนุญาตตามนโยบายจะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๒๘.๔ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต ผู้ดูแลระบบจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๒๘.๕ การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๒๘.๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยต้องกำหนดให้มีการจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๒๘.๗ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย และจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลอย่างน้อยดังนี้

๒๘.๗.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๒๘.๗.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๒๘.๗.๓ วัตถุประสงค์หรือชื่อแอปพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

๒๘.๗.๔ วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

๒๘.๘ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

/๒๘.๙ การเชื่อมต่อ ...

๒๘.๙ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน ผู้ดูแลระบบจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมายจาก สศค. ก่อนทุกครั้ง

๒๙. นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS Policy)

<u>วัตถุประสงค์</u>

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่ายเพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายใน สศค. ให้มีความมั่นคงปลอดภัย

๒๙.๑ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของ สศค. และเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๒๙.๒ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๒๙.๓ ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๒๙.๔ โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๒๙.๕ มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS อย่างสม่ำเสมอ

๒๙.๖ มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๒๙.๗ IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

๒๙.๘ เครื่องคอมพิวเตอร์แม่ข่ายที่มีการติดตั้ง Host - Based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๒๙.๙ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย กิจกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ รวมถึงระบบมีการทำงานที่ผิดปกติ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีหรือภายใน ๑ ชั่วโมงที่ตรวจพบ

๒๙.๑๐ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

/๒๙.๑๑ มีรูปแบบ ...

๒๙.๑๑ มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ

ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ เพื่อป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๒๙.๑๒ สศค. สงวนสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๒๙.๑๓ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ สศค. การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของ สศค. จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๓๐. นโยบายการบริหารจัดการความต่อเนื่องของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการบริหารจัดการระบบสำรองสำหรับระบบสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน (Incident) หรือกรณีเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๓๐.๑ ต้องมีแผนสำรองข้อมูล โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๓๐.๑.๑ คัดเลือกระบบสารสนเทศที่สำคัญและมีความจำเป็นเพื่อจัดทำระบบสำรอง โดยเก็บสำรองข้อมูลไว้ที่ศูนย์สำรองข้อมูล (DR Site) ภายนอกสถานที่อย่างน้อย ๑ ชุด

๓๐.๑.๒ กำหนดรายละเอียดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ ประกอบด้วยข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการและซอฟแวร์อื่น ๆ ที่เกี่ยวข้อง เป็นต้น

๓๐.๑.๓ กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูล โดยแยกตามระบบเทคโนโลยีสารสนเทศแต่ละระบบ

๓๐.๑.๔ กำหนดวิธีการสำรองที่เหมาะสมกับระบบงานโดยคำนึงถึงความสำคัญของระบบงานและข้อมูลสารสนเทศของระบบงานนั้น ได้แก่ สำรองแบบทั้งหมด (Full Backup) สำรองเพียงบางส่วน (Incremental Backup) หรือทั้งสองแบบ

๓๐.๑.๕ เตรียมอุปกรณ์ที่จำเป็นต่อการสำรองข้อมูล และการกู้คืนข้อมูล

/๓๐.๑.๖ ระยะความถี่ ...

๓๐.๑.๖ ระยะความถี่การสำรองข้อมูลของระบบงานขึ้นอยู่กับความสำคัญของระบบ และ

สภาพการเปลี่ยนแปลงของระบบงานนั้น ๆ โดยระบบงานที่มีการเปลี่ยนแปลงบ่อยต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๓๐.๑.๗ สำรองข้อมูลตามชนิด ระยะความถี่ และวิธีการสำรองที่ได้กำหนดไว้ พิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล ผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๓๐.๑.๘ ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไว้นั้นมีความครบถ้วน

๓๐.๒ ต้องมีแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อรองรับภัยพิบัติและสถานการณ์ฉุกเฉินระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๓๐.๒.๑ ระบุวัตถุประสงค์หลักของแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓๐.๒.๒ จัดทำบัญชีรายชื่อของระบบงานที่มีความสำคัญรวมทั้งปรับปรุงบัญชีรายชื่อดังกล่าวให้มีความทันสมัยอยู่เสมอ

๓๐.๒.๓ กำหนดปัจจัยเสี่ยงและภัยพิบัติที่อาจส่งผลกระทบกับระบบงานที่สำคัญและกำหนดมาตรการเพื่อลดความเสี่ยงที่พบในกรณีต่าง ๆ ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

๓๐.๒.๔ ประเมินสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓๐.๓ ต้องมีแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan: IT DRP) เพื่อรับมือกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๓๐.๓.๑ กำหนดหน้าที่ความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

๓๐.๓.๒ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน โดยมีแนวทางและข้อปฏิบัติตามแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อรองรับภัยพิบัติและสถานการณ์ฉุกเฉินระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๓๐.๓.๓ กำหนดช่องทางการติดต่อกับผู้ให้บริการภายนอก หรือผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เมื่อเกิดเหตุจำเป็นต้องติดต่อ

๓๐.๓.๔ สร้างความตระหนักรู้หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติเมื่อเกิดเหตุหรือสถานการณ์ฉุกเฉิน

๓๐.๓.๕ ปรับปรุงแผนกู้คืนอย่างน้อยปีละ ๑ ครั้ง

๓๐.๓.๖ จัดประชุมและแจ้งให้ผู้เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งเมื่อมีการปรับปรุงแผนกู้คืนใหม่

/๓๐.๔ กำหนด ...

๓๐.๔ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ระบุไว้ในแผนบริหารความเสี่ยงเพื่อความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ แผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อรองรับภัยพิบัติและสถานการณ์ฉุกเฉินระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) แผนสำรองข้อมูลและแผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan: IT DRP)

๓๐.๕ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง แผนสำรองข้อมูล แผนกู้คืนระบบเทคโนโลยีสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓๐.๕.๑ ตรวจสอบว่าระบบสำรองที่เกิดขึ้นนั้นได้กระทำสำเร็จครบถ้วนหรือไม่

๓๐.๕.๒ ทดสอบกู้คืนข้อมูลที่สำรองไว้และความพร้อมใช้งาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้อย่างครบถ้วนภายในระยะเวลาที่เหมาะสม หากพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ต้องดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีแก้ไขอย่างเป็นลายลักษณ์อักษร

๓๐.๕.๓ ตรวจสอบ ทบทวน ประเมินผล และทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง แผนสำรองข้อมูล แผนกู้คืนระบบเทคโนโลยีสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อซักซ้อมกระบวนการในการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่ามาตรการที่กำหนดสามารถใช้ได้ผลและถูกต้องเมื่อมีเหตุการณ์ที่ทำให้หยุดชะงักเกิดขึ้น

๓๐.๕.๔ ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๓๑. นโยบายความมั่นคงปลอดภัยด้านบุคลากร (Human Security Policy)

<u>วัตถุประสงค์</u>

เพื่อให้มั่นใจว่าบุคลากรและบุคคลที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยมีทักษะ ความรู้และความสามารถเพียงพอ รวมถึงมีความตระหนักในการปฏิบัติงานอย่างมั่นคงปลอดภัย

๓๑.๑ กำหนดและมอบหมายหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ โดยแบ่งแยกหน้าที่ความรับผิดชอบอย่างเหมาะสม

๓๑.๒ จัดทำและปรับปรุงรายชื่อข้อมูลติดต่อหน่วยงานผู้มีอำนาจกำกับดูแลด้านความมั่นคงปลอดภัย เครือข่ายหรือกลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศเพื่อสะดวกในการติดต่อประสานงานและรับทราบข่าวสารด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นปัจจุบัน

/๓๑.๓ มีกระบวนการ ...

๓๑.๓ มีกระบวนการคัดเลือกและตรวจสอบภูมิหลังของผู้สมัครงานให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ และจริยธรรมที่เกี่ยวข้อง โดยต้องดำเนินการในระดับที่เหมาะสมกับความต้องการของ สศค. ชั้นความลับของข้อมูลที่จะถูกเข้าถึงและความเสี่ยงที่เกี่ยวข้อง

๓๑.๔ ในการทำข้อตกลงและเงื่อนไขในสัญญาจ้างกับบุคลากรและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรของผู้ที่ทำสัญญาจ้าง และข้อตกลงการไม่เปิดเผยความลับ

๓๑.๕ เมื่อสิ้นสุดหรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน รวมถึงต้องคืนทรัพย์สินและสิทธิ์ในการเข้าถึงระบบต่าง ๆ ของ สศค.

๓๑.๖ เผยแพร่และแจ้งเวียนประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สศค. รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้องให้แก่บุคลากรทั้งภายในและภายนอก สศค.

๓๑.๗ จัดฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) หรือหลักสูตรอื่นที่เกี่ยวข้องเพื่อเสริมสร้างความรู้ความเข้าใจ วิธีการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์อย่างมั่นคงปลอดภัยให้กับบุคลากรผู้ใช้งานเกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบ รวมถึงการป้องกันการกระทำผิดจากการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ หรือการกระทำที่ขัดต่อข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดของ สศค.

๓๑.๘ จัดฝึกอบรมการใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการพัฒนาระบบสารสนเทศขึ้นมาใช้งานหรือมีการปรับปรุง/ปรับเปลี่ยนการใช้งานของระบบสารสนเทศที่มีนัยสำคัญ

๓๑.๙ จัดฝึกอบรมปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สศค. รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้องให้แก่บุคลากรของ สศค. อย่างสม่ำเสมอ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมประจำปีของ สศค.

๓๑.๑๐ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมถึงนโยบายอื่น ๆ ที่เกี่ยวข้องเพื่อสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรของ สศค. โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๓๑.๑๑ ประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๓๑.๑๒ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

/๓๒. นโยบาย ...

๓๒. นโยบายการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (Project Management Policy)

<u>วัตถุประสงค์</u>

เพื่อควบคุมการบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศได้อย่างมั่นคงปลอดภัย ตั้งแต่ก่อนเริ่มจัดทำโครงการจนกระทั่งโครงการเสร็จสิ้นและลดผลกระทบจากการดำเนินงานโครงการที่อาจส่งผลกระทบต่อระบบสารสนเทศของ สศค.

๓๒.๑ ระบุวัตถุประสงค์ด้านความมั่นคงปลอดภัยไว้ในแต่ละโครงการ

๓๒.๒ กำหนดแผนดำเนินการโครงการ

๓๒.๓ ก่อนการจัดทำโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ผู้รับผิดชอบโครงการต้องดำเนินการประเมินความเสี่ยงของโครงการที่มีผลกระทบต่อระบบสารสนเทศของ สศค. และระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งจัดให้มีการบริหารจัดการความเสี่ยงที่เกิดขึ้น

๓๒.๔ ผู้รับผิดชอบโครงการพิจารณาเลือกแนวทางตามหลักการวิศวกรรมระบบที่น่าเชื่อถือและมีความมั่นคงปลอดภัยตามหลักการวิศวกรรมสำหรับการพัฒนาระบบให้เกิดความมั่นคงปลอดภัย และ/หรือ ข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Security Requirements) รวมถึงแนวคิด Data Protection by Design & Design เพื่อควบคุมการปฏิบัติงานที่เกี่ยวกับข้อมูลส่วนบุคคลให้มีความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ ๒๕๖๒ มาเป็นแนวทางในการดำเนินการประยุกต์เข้ากับโครงการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ หากการดำเนินการโครงการดังกล่าวมีการจ้างผู้ให้บริการภายนอกเข้ามาดำเนินการจะต้องแจ้งผู้ให้บริการภายนอกปฏิบัติตามหลักการวิศวกรรมระบบและแนวคิด Data Protection by Design & Design สำหรับการพัฒนาระบบให้เกิดความมั่นคงปลอดภัยด้วย

๓๓. นโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางบริหารจัดการทรัพย์สินสารสนเทศในขอบเขตระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศตั้งแต่การลงทะเบียนทรัพย์สิน ระบุหน้าที่ความรับผิดชอบอย่างเหมาะสม การป้องกันข้อมูลและสารสนเทศตามระดับที่กำหนดไว้ให้สอดคล้องกับระดับความสำคัญของทรัพย์สินนั้น ๆ รวมถึงมีการป้องกันไม่ให้มีการเปิดเผย แก้ไข เคลื่อนย้ายหรือกำจัดข้อมูลและสารสนเทศที่เก็บไว้ในสื่อบันทึกโดยไม่ได้รับอนุญาต

๓๓.๑ หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศของ สศค.

๓๓.๑.๑ ศูนย์เทคโนโลยีสารสนเทศต้องดำเนินการจัดทำทะเบียนทรัพย์สินและมีการปรับปรุงทะเบียนทรัพย์สินให้ถูกต้อง ทันสมัยอยู่เสมอ ซึ่งทะเบียนทรัพย์สินต้องครอบคลุมทรัพย์สินแต่ละประเภท คือ ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บริการ บุคลากร Virtual Machine (VM)

/๓๓.๑.๒ ทรัพย์สิน ...

๓๓.๑.๒ ทรัพย์สินต่าง ๆ ที่อยู่ในทะเบียนทรัพย์สินต้องมีการระบุผู้ที่เป็นเจ้าของเพื่อกำหนดความรับผิดชอบในการบริหารจัดการทรัพย์สินอย่างเหมาะสม

๓๓.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง และต้องปรับปรุงทะเบียนทรัพย์สินหากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของ สศค.

๓๓.๒ การจัดชั้นความลับของสารสนเทศ

๓๓.๒.๑ กำหนดประเภทของข้อมูลและสารสนเทศที่กำหนดชั้นความลับ (Confidential Data and Information) โดยพิจารณาข้อกำหนดด้านกฎหมาย คุณค่า ระดับความสำคัญและความลับของข้อมูลและสารสนเทศ หากถูกเปิดเผยออกไปแล้วจะมีความเสี่ยงที่ก่อให้เกิดความเสียหายหรือเกิดผลเสียอื่น ๆ ต่อ สศค. ต้องกำหนดประเภทของข้อมูล จัดแบ่งลำดับความสำคัญของข้อมูล จัดแบ่งลำดับชั้นความลับของข้อมูล จัดแบ่งระดับชั้นการเข้าถึง กำหนดเวลาเข้าถึงได้ และกำหนดช่องทางการเข้าถึงสำหรับสารสนเทศ รวมถึงกำหนดให้บุคลากรปฏิบัติตามให้สอดคล้องกับขั้นตอนการจัดชั้นความลับและการจัดการข้อมูลและสารสนเทศที่ สศค. กำหนดไว้ อย่างเคร่งครัด

(๑) กำหนดประเภทของข้อมูล ดังนี้

(๑.๑) ข้อมูลและสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(๑.๒) ข้อมูลและสารสนเทศที่ให้บริการหรือเผยแพร่ ได้แก่ ข้อมูลด้านเศรษฐกิจการเงิน การคลัง เป็นต้น

(๒) จัดแบ่งลำดับความสำคัญของข้อมูล ดังนี้

(๒.๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒.๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๒.๓) ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้

(๓.๑) กำหนดบุคคลผู้ทำหน้าที่เป็นผู้บริหารจัดการสารสนเทศภายในหน่วยงานเป็นผู้ทำหน้าที่จัดหมวดหมู่ทรัพย์สินสารสนเทศ ได้แก่ ข้อมูลดิจิทัล (Digital Data) หรือสารสนเทศดิจิทัล (Digital Information) โดยระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และต้องมีการจัดลำดับชั้นความลับเป็นอย่างหนึ่งอย่างใดต่อไปนี้

/(๑) “ชั้นลับ ...

(๑) “ชั้นลับที่สุด”

(๒) “ชั้นลับมาก”

(๓) “ชั้นลับ”

(๔) “ชั้นไม่ลับ หรือ ชั้นเปิดเผย”

กำหนดให้บุคลากรประจำหน่วยงานเป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานในการจัดเก็บข้อมูลและสารสนเทศที่อยู่ในชั้นไม่ลับหรือชั้นเปิดเผยนี้ เข้าสู่ระบบบริหารจัดการองค์ความรู้ (Knowledge Management System) หรือระบบจัดเก็บเอกสาร (Document Image System) ตามความเหมาะสม โดยให้เลขานุการกรม ผู้อำนวยการกอง/กลุ่ม/ศูนย์ พิจารณาอนุมัติในแบบฟอร์มการจัดเก็บทรัพย์สินสารสนเทศก่อนทุกครั้ง

(๓.๒) เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

(๓.๓) ให้บุคลากรประจำหน่วยงานเป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันสารสนเทศของ สศค. ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย สศค. จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศ กำหนดให้มีชั้นความลับที่สุด ชั้นลับมาก ชั้นลับ และชั้นไม่ลับ หรือชั้นเปิดเผย การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูลของ สศค. ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสม ไม่ว่าจะอยู่ ในรูปแบบใดก็ตาม มีการกำหนดชั้นความลับ ดังนี้

/(๓.๓.๑) ชั้นลับที่สุด ...

(๓.๓.๑) ชั้นลับที่สุด กำหนดให้มีระดับความปลอดภัยที่ ๔ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อ สศค. มากที่สุด ต้องได้รับการรักษาความลับของเนื้อหาโดยการเข้ารหัสอย่างยาก (Strong Encryption) และจำกัดการเข้าถึง (Access Control) เป็นอย่างดี ได้แก่ Private Key ของ สศค. หรือข้อมูลที่ได้จากการประชุมที่มีมติที่ประชุมกำหนดให้เป็นชั้นความลับนี้ ตัวอย่างข้อมูลชั้นลับที่สุด ได้แก่ นโยบายหรือแผนที่สำคัญยิ่งของ สศค. ซึ่งถ้าเปิดเผยก่อนเวลาอันสมควร อาจก่อให้เกิดผลเสียหายอย่างร้ายแรงแก่ สศค. แผนยุทธศาสตร์ที่เกี่ยวกับข้อมูลสำคัญในการปฏิบัติภารกิจของ สศค. ร่วมกับหน่วยงานอื่น เอกสารของ สศค. ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เป็นต้น

(๓.๓.๒) ชั้นลับมาก กำหนดให้มีระดับความปลอดภัยที่ ๓ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อ สศค. มาก ต้องได้รับการรักษาความลับของเนื้อหาโดยการเข้ารหัส (Encryption) หรือจำกัดการเข้าถึง (Access Control) ตัวอย่างข้อมูลชั้นลับมาก ได้แก่ รายงานเสนอการแต่งตั้ง ถอดถอนหรือโยกย้ายพนักงานในตำแหน่งที่สำคัญมาก การเจรจาข้อตกลงที่สำคัญกับหน่วยงานอื่น เทคนิคที่ต้องอาศัยความชำนาญพิเศษ เป็นต้น

(๓.๓.๓) ชั้นลับ กำหนดให้มีระดับความปลอดภัยที่ ๒ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อ สศค. โดยจำกัดการเข้าถึง (Access Control) ตัวอย่างข้อมูลชั้นลับ ได้แก่ การดำเนินการที่เกี่ยวกับการเปลี่ยนแปลงตำแหน่งที่สำคัญใน สศค. ระเบียบวาระการประชุมลับ ประกาศหรือคำสั่งที่สำคัญที่อยู่ระหว่างการดำเนินการ เป็นต้น

(๓.๓.๔) ชั้นไม่ลับ หรือ ชั้นเปิดเผย กำหนดให้มีระดับความปลอดภัยที่ ๑ สำหรับข้อมูลและสารสนเทศที่ไม่มีความลับ สามารถเผยแพร่ได้ ตัวอย่างข้อมูลชั้นไม่ลับ หรือชั้นเปิดเผย ประกอบด้วย ข้อมูลและสารสนเทศที่เป็นความรู้ของ สศค. ในลักษณะงานวิจัย นโยบาย ข้อกฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา พระราชกำหนด ข้อมูลและสารสนเทศที่เป็นประกาศ คำสั่งแต่งตั้ง ข่าวประชาสัมพันธ์

/(๓.๔) ข้อมูลที่ ...

(๓.๔) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลายและกำหนดเป็นระเบียบปฏิบัติให้ข้าราชการและลูกจ้างของ สศค. ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

(๔) จัดแบ่งระดับชั้นการเข้าถึง

(๔.๑) ผู้ดูแลบริหารจัดการระบบ (Administrator) ต้องได้รับสิทธิ์ในการเข้าใช้งานจากศูนย์เทคโนโลยีสารสนเทศ โดยมีการกำหนด User และ Password ในการเข้าใช้งานโดยผ่านทาง Secure Shell ซึ่งแยกประเภทตามความรับผิดชอบ ได้แก่ Network Admin, System Admin และ Database Admin

(๔.๒) ผู้ใช้งานต้องได้รับสิทธิ์ในการเข้าใช้งานจากศูนย์เทคโนโลยีสารสนเทศ โดยต้องใช้งานผ่านระบบ Single Sign - On ของ สศค. และต้องใช้ User และ Password เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

(๕) กำหนดเวลาเข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

(๖) กำหนดช่องทางการเข้าถึงสำหรับสารสนเทศอย่างเคร่งครัด

ผู้ได้รับสิทธิ์ต้องทำการ Log In ด้วย User และ Password ผ่านระบบ Single Sign - On เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

๓๓.๓ การจัดการสื่อบันทึกข้อมูล

๓๓.๓.๑ ห้ามใช้งานสื่อบันทึกข้อมูลที่สามารถอ่านเขียนข้อมูลอิเล็กทรอนิกส์และเคลื่อนย้ายได้ ยกเว้นสื่อบันทึกที่ได้รับอนุญาตให้ใช้งานโดยผู้บังคับบัญชาของส่วนงาน

๓๓.๓.๒ ต้องตรวจสอบให้แน่ใจว่ามีการควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูล โดยใช้มาตรการอย่างน้อย ดังนี้

- ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลและอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ตรวจสอบว่าสื่อบันทึกข้อมูลและอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีโปรแกรมไม่ประสงค์ดีก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของ สศค.

/๓๓.๓.๓ ข้อมูล ...

๓๓.๓.๓ ข้อมูลที่บันทึกอยู่ในสื่อบันทึกข้อมูลที่สามารถอ่านเขียนข้อมูลอิเล็กทรอนิกส์และเคลื่อนย้ายได้ต้องถูกทำลายด้วยวิธีการที่ไม่สามารถกู้คืนได้ทันทีที่ไม่มีความจำเป็นต้องใช้งานข้อมูลนั้น

๓๓.๓.๔ สื่อบันทึกข้อมูลต้องได้รับการจัดเก็บในสภาพแวดล้อมที่เหมาะสมตามที่ผู้ผลิตสื่อกำหนด

๓๓.๓.๕ กรณีสื่อบันทึกที่มีวันหมดอายุ เช่น เทปแม่เหล็ก (Backup tape) ต้องถ่ายโอนข้อมูลออกสื่อบันทึกเดิมและทำลายสื่อบันทึกดังกล่าวด้วยวิธีการทำลายที่กำหนดไว้

๓๓.๓.๖ อุปกรณ์อ่านเขียนหรือช่องทางในการเชื่อมต่อกับสื่อบันทึกข้อมูลที่สามารถอ่านเขียนข้อมูลอิเล็กทรอนิกส์และเคลื่อนย้ายได้ต้องถูกถอดถอนออกจากเครื่องคอมพิวเตอร์หรือปิดกั้นการใช้งานด้วยวิธีการที่เหมาะสม ยกเว้นกรณีที่มีความจำเป็นต้องใช้งานสื่อบันทึกเพื่อการปฏิบัติงานเท่านั้น

๓๓.๓.๗ สื่อบันทึกที่หมดอายุการใช้งานหรือหมดความจำเป็นในการใช้งานและต้องการกำจัดทิ้ง ต้องถูกทำลายด้วยวิธีการที่เหมาะสมที่ไม่สามารถกู้คืนข้อมูลได้ เพื่อป้องกันข้อมูลรั่วไหล และการนำกลับมาใช้ใหม่ ตามแนวทางการทำลายข้อมูลและสื่อบันทึกดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๓๓.๓.๘ กรณีที่ใช้บริการทำลายสื่อบันทึกจากผู้ให้บริการภายนอกต้องเลือกใช้บริการจากผู้ให้บริการที่มีประสบการณ์และมีความน่าเชื่อถือเท่านั้น รวมถึงต้องดำเนินการตรวจสอบความเหมาะสมของเครื่องมือและขั้นตอนการดำเนินการของผู้ให้บริการก่อนตกลงใช้บริการ

๓๓.๓.๙ สื่อบันทึกข้อมูลสำคัญ ได้แก่ สื่อบันทึกข้อมูลสำรองทุกประเภท เอกสารและสื่อบันทึกข้อมูลระดับลับ (Confidential) เอกสารที่มีข้อมูลส่วนบุคคล เอกสารสัญญาและข้อตกลง เอกสารและข้อมูลที่ถือเป็นทรัพย์สินทางปัญญา และเอกสารหรือสื่อบันทึกที่มีข้อมูลที่ถูกควบคุมโดยข้อกำหนดของกฎหมายหรือข้อบังคับใด ๆ ต้องถูกบันทึก

/รายละเอียด ...

รายละเอียดของการทำลายทุกครั้ง โดยต้องบันทึกข้อมูลอย่างน้อย ได้แก่ รายละเอียดของสื่อบันทึกและข้อมูลภายใน เหตุผลในการทำลาย วิธีการทำลาย วันเวลาที่ทำลาย ผู้ดำเนินการและผู้อนุมัติ

๓๓.๓.๑๐ ในกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูล สื่อบันทึกที่มีข้อมูลเหล่านั้นต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์หรือการถูกทำให้เกิดความเสียหายในระหว่างการขนย้าย

๓๓.๓.๑๑ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของ สศค. บนสื่อบันทึกข้อมูล

๓๔. นโยบายการถ่ายโอนสารสนเทศ (Information Transfer Policy)

<u>วัตถุประสงค์</u>

กำหนดแนวทางและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures) สำหรับการถ่ายโอนสารสนเทศของ สศค. เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายใน สศค. และถ่ายโอนกับหน่วยงานภายนอก

๓๔.๑ แนวทางข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreement) สำหรับการถ่ายโอนสารสนเทศของ สศค. ให้มีความมั่นคงปลอดภัย

๓๔.๑.๑ กำหนดขั้นตอนปฏิบัติและมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง ซึ่งต้องครอบคลุมมาตรฐานทางเทคนิคสำหรับการบันทึกและการอ่านข้อมูล มาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์ มาตรฐานทางเทคนิคสำหรับการบรรจุและรับส่ง

๓๔.๑.๒ กำหนดการบริหารจัดการการควบคุม กำหนดขั้นตอนปฏิบัติในการแลกเปลี่ยนข้อมูล (การรับ - ส่งข้อมูล) รวมถึงหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการป้องกันข้อมูล การแจ้งรับ - ส่งข้อมูล การจัดส่งข้อมูล และการรับข้อมูลให้ชัดเจน

๓๔.๑.๓ กำหนดขั้นตอนการตรวจสอบย้อนกลับสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูลเพื่อเป็นการป้องกันการปฏิเสธความรับผิดชอบ

๓๔.๑.๔ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญเสียหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๓๔.๑.๕ กำหนดความรับผิดชอบในกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยข้อมูลรวมถึงการละเมิดข้อมูลส่วนบุคคล

๓๔.๑.๖ กำหนดสิทธิ์การเข้าถึงข้อมูลและระดับที่ยอมรับได้ของมาตรการควบคุมการเข้าถึง

๓๔.๑.๗ การใช้งานระบบการติดป้ายสำหรับข้อมูลที่สำคัญเพื่อให้มั่นใจว่าวิธีการติดป้ายสามารถเข้าใจได้ในทันทีและข้อมูลต้องมีการป้องกันอย่างเหมาะสม

/๓๔.๑.๘ กำหนด ...

๓๔.๑.๘ กำหนดวิธีการทางเทคนิคหรือมาตรการควบคุมพิเศษใด ๆ ที่จำเป็นต้องใช้สำหรับป้องกันเอกสารที่มีความสำคัญ ข้อมูลลับ ข้อมูลส่วนบุคคล รวมถึงข้อมูลอ่อนไหว ซอฟต์แวร์ หรือข้อมูลอื่น ๆ ที่มีความสำคัญจากการถูกเข้าถึง ถูกเปลี่ยนแปลง ถูกแก้ไข ถูกสวมรอยโดยผู้อื่น ถูกเปิดเผยความลับโดยไม่ได้รับอนุญาต เช่น การใช้กุญแจที่ใช้ในการเข้ารหัส (Token Key) หรือการใช้เทคนิคพิเศษในการเข้ารหัสข้อมูล หรือการแปลงรหัส

๓๔.๑.๙ การรักษาห่วงโซ่ของการปกป้องข้อมูลในขณะการรับ - ส่งข้อมูล (Chain of Custody) เพื่อรักษาความปลอดภัยและความถูกต้องของข้อมูล โดยควบคุมและติดตามข้อมูลอย่างต่อเนื่องตลอดกระบวนการรับ – ส่งข้อมูล ให้มั่นใจได้ว่าข้อมูลได้รับการจัดการอย่างถูกต้องและปลอดภัย ไม่มีการบุกรุก สูญหาย หรือเสียหาย หรือถูกเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๓๔.๑.๑๐ กำหนดแนวทางที่เหมาะสมเกี่ยวกับการใช้งานระบบหรืออุปกรณ์ที่ใช้ในการสื่อสารข้อมูลระหว่าง สศค. กับหน่วยงานภายนอก โดยห้ามใช้เพื่อก่อความรำคาญแก่ผู้อื่น หรือทำให้ผู้อื่นสูญเสียชื่อเสียง หรือการปลอมเป็นบุคคลอื่น

๓๔.๑.๑๑ กำหนดแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ที่สอดคล้องกับกฎหมาย ระเบียบข้อบังคับ รวมถึงนโยบายที่ สศค. กำหนด

๓๔.๒ การบริหารจัดการการใช้ข้อมูลร่วมกัน

กำหนดแนวทางการรักษาความมั่นคงปลอดภัยเพื่อบริหารจัดการและควบคุมการใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกันระหว่าง สศค. หรือหน่วยงานที่ประสงค์จะเชื่อมโยง

๓๔.๒.๑ กำหนดมาตรการที่เหมาะสมเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๓๔.๒.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๓๔.๒.๓ พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรืออนุญาตให้เข้าใช้งาน

๓๔.๒.๔ พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๓๔.๒.๕ ไม่อนุญาตให้ใช้งานข้อมูลสำคัญหรือลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันที่เพียงพอและเหมาะสม

๓๔.๓ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit Logging)

กำหนดให้มีการบันทึกข้อมูลพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ ดังนี้

/๓๔.๓.๑ ข้อมูล ...

๓๔.๓.๑ ข้อมูลชื่อบัญชีผู้ใช้
๓๔.๓.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ
๓๔.๓.๓ ข้อมูลวันเวลาที่ออกจากระบบ
๓๔.๓.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
๓๔.๓.๕ ข้อมูลชื่อเทอร์มินัล
๓๔.๓.๖ ข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ
๓๔.๓.๗ ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
๓๔.๓.๘ ข้อมูลการเปลี่ยนคอนฟิกูเรชัน (Configurations) ของระบบ
๓๔.๓.๙ ข้อมูลแสดงการใช้สิทธิ์ของผู้ดูแลระบบ
๓๔.๓.๑๐ ข้อมูลแสดงการใช้งานแอปพลิเคชั่น
๓๔.๓.๑๑ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ ได้แก่ เปิด ปิด เขียน อ่านไฟล์
๓๔.๓.๑๒ ข้อมูล IP Address ที่เข้าถึง
๓๔.๓.๑๓ ข้อมูลโปรโตคอลเครือข่ายที่ใช้
๓๔.๓.๑๔ ข้อมูลการแจ้งเตือนเกี่ยวกับการเข้าถึงระบบ
๓๔.๓.๑๕ ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
๓๔.๓.๑๖ ข้อมูลแสดงการหยุดการทำงานของระบบงานสำคัญ ๆ
๓๔.๓.๑๗ ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๓๕. นโยบายด้านการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management Policy & Procedure)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมกระบวนการจัดหาระบบงานสารสนเทศใหม่ที่เกี่ยวข้องกับการพัฒนาระบบงานสารสนเทศ และ/หรือ การปรับปรุงเปลี่ยนแปลงระบบงานสารสนเทศที่ใช้งานอยู่ ให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลในกระบวนการจัดหาหรือพัฒนาระบบสารสนเทศ รวมถึงให้มีการปกป้องข้อมูลที่จะนำไปใช้ในการทดสอบระบบสารสนเทศให้มีความถูกต้องและน่าเชื่อถือ (Integrity) และมีความพร้อมใช้งาน (Availability)

๓๕.๑ มาตรการในการบริหารจัดการเพื่อควบคุมการพัฒนาหรือปรับปรุงระบบสารสนเทศ กำหนดแนวทางดังนี้

๓๕.๑.๑ กำกับดูแล ขั้นตอน กระบวนการจัดหาระบบงานสารสนเทศใหม่ที่เกี่ยวข้องกับการพัฒนาระบบงานสารสนเทศและการปรับปรุงเปลี่ยนแปลงระบบงานสารสนเทศ (Change Management Policy & Procedure) ตามวงจรการพัฒนาระบบงาน (System Development Life Cycle: SDLC) ดังนี้

/(๑) การค้นหา ...

(๑) การค้นหาปัญหาของ สศค. (Problem Recognition)

บุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับบุคลากรของสำนักงาน/กอง/กลุ่ม/ศูนย์ ในการกำหนดปัญหา (Problem Definition) ที่เกิดขึ้นและจำเป็นต้องพัฒนาระบบงานเพื่อแก้ปัญหานั้น

(๒) การศึกษาความเหมาะสม (Feasibility Study)

มีการวางแผนและการสำรวจความต้องการของผู้ใช้งาน โดยบุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับผู้เกี่ยวข้องทำการศึกษา และ/หรือ ทดสอบความเป็นไปได้ในการนำเครื่องมือและอุปกรณ์มาประยุกต์ใช้ในการพัฒนาระบบงานสารสนเทศให้มีประสิทธิภาพและทันสมัย รวมถึงกำหนดให้มีการดำเนินการและจัดทำเอกสารที่สำคัญโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ มีข้อกำหนดขอบเขตของงาน (Term of Reference: TOR) ที่ชัดเจน ประกอบด้วย หลักการ เหตุผลความจำเป็น เป้าหมาย วัตถุประสงค์ รายละเอียดคุณลักษณะเฉพาะของฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงระบบงานที่จะปรับปรุงหรือพัฒนาขึ้นใหม่

๒.๒ มีแผนการดำเนินงานโครงการ (Activity Schedule Plan) ที่ระบุกิจกรรมและระยะเวลาเริ่มต้น – สิ้นสุด ในแต่ละกิจกรรม

๒.๓ มีการสำรวจเบื้องต้นและจัดทำเอกสารสรุปความต้องการของผู้ใช้ (User Requirements)

๒.๔ กำหนดลักษณะประเภท รูปแบบข้อมูล แหล่งข้อมูล วิธีการจัดเก็บและนำเข้าข้อมูล ความถี่ในการปรับปรุงข้อมูล เงื่อนไขต่าง ๆ การนำข้อมูลไปใช้งาน

(๓) การวิเคราะห์และการออกแบบ (Analysis and Design)

บุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับบุคลากรของสำนักงาน/กอง/กลุ่ม/ศูนย์ ในการให้ข้อมูลที่จำเป็นต้องใช้สำหรับการวิเคราะห์และออกแบบระบบงานแก่ผู้ให้บริการภายนอก (Outsource) กำหนดให้มีการดำเนินการและจัดทำเอกสารที่สำคัญโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๓.๑ มีการสำรวจความต้องการของผู้ใช้ และจัดทำเอกสารสรุปความต้องการของผู้ใช้ (User Requirements) เพื่อให้ครอบคลุมเนื้องานอีกครั้ง

๓.๒ มีการจัดทำเอกสารการวิเคราะห์และออกแบบระบบงาน (System Analysis and System Design) ครอบคลุมทุกระบบงานตาม TOR และ User Requirements ล่าสุด

๓.๓ มีการจัดทำเอกสารแสดง ER Diagram หรือ Flowchart ที่แสดงถึงกระบวนการทำงาน (Procedure) และการไหลของข้อมูล (Data Flow) ของระบบงาน

/(๔) การพัฒนา ...

(๔) การพัฒนาและทดสอบ (Development and Testing)

บุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับบุคลากรของสำนักงาน/กอง/กลุ่ม/ศูนย์ ในการสนับสนุนในการพัฒนาและการทดสอบระบบงาน กำหนดให้มีการดำเนินการและจัดทำเอกสารที่สำคัญโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๔.๑ มีการจัดทำระบบต้นแบบ (Prototype) เพื่อให้ผู้ใช้งานสามารถมองเห็นการทำงานของระบบในภาพรวมก่อนการพัฒนาจริง

๔.๒ มีการรายงานผลการทดสอบความถูกต้องและการยอมรับได้ของระบบงาน (Acceptance Test) โดยมีการทดสอบที่ครอบคลุม Unit Test, System Test, System Integrated Test (SIT), User Acceptance Test (UAT), Operation Acceptance Test (OAT) หรือเลือกวิธีใดวิธีหนึ่งตามความเหมาะสมของระบบ

๔.๓ การควบคุมการทดสอบ

๔.๓.๑ ต้องกำหนดให้มีการทดสอบหน่วย (Unit Test) ในระหว่างการพัฒนาระบบเพื่อทดสอบการทำงานของแต่ละส่วนเพื่อให้มั่นใจว่าแต่ละส่วนไม่มีข้อผิดพลาด สามารถใช้งานได้ตามความต้องการ ก่อนที่จะทำการทดสอบในลำดับถัดไป

๔.๓.๒ ต้องกำหนดให้มีการทดสอบการทำงานของฟังก์ชั่นในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อมูลส่วนบุคคล รวมถึงข้อมูลอ่อนไหวตั้งแต่ระบบสารสนเทศนั้นอยู่ระหว่างการพัฒนาหรืออยู่ระหว่างการปรับปรุงเปลี่ยนแปลงเพื่อให้มั่นใจว่าฟังก์ชั่นในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ข้อมูลส่วนบุคคล รวมถึงข้อมูลอ่อนไหวสามารถทำงานได้ตามความต้องการ

๔.๓.๓ ต้องกำหนดให้มีการทดสอบระบบก่อนนำไปใช้งาน (System acceptance testing) ทั้งระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่และที่มีการปรับปรุงเปลี่ยนแปลง โดยนำผลที่ได้จากการทดสอบมาเทียบกับเกณฑ์สำหรับใช้ในการทดสอบระบบที่เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศได้เตรียมไว้

๔.๓.๔ ต้องกำหนดให้มีการควบคุมการเข้าถึง การใช้งาน การจัดเก็บ และทำลายข้อมูลที่ใช้ในการทดสอบเพื่อป้องกันการรั่วไหลของข้อมูลทดสอบและความเสี่ยงต่าง ๆ อาจเกิดขึ้นเมื่อข้อมูลทดสอบรั่วไหลและถูกเข้าถึงโดยไม่ได้รับอนุญาต

/(๕) การติดตั้ง ...

(๕) การติดตั้งใช้งาน (Implementation)

บุคลากรของศูนย์เทคโนโลยีสารสนเทศให้การสนับสนุนในการติดตั้งระบบงาน กำหนดกระบวนการควบคุมตามขั้นตอนโดยให้มีการดำเนินการและจัดทำเอกสารที่สำคัญโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๕.๑ การติดตั้งระบบ

๕.๑.๑ ติดตั้งซอฟต์แวร์และระบบงานที่พัฒนาขึ้นทั้งหมด

๕.๑.๒ นำระบบงานที่พัฒนาสมบูรณ์แล้วทั้งหมดออกปฏิบัติงานจริง (Overall Implementation)

๕.๒ การควบคุมเชิงป้องกัน (Preventive control)

๕.๒.๑ มีแผนการฝึกอบรมที่ประกอบด้วยจำนวนหลักสูตรที่จำเป็นต่อการใช้ระบบครอบคลุมทั้งผู้ใช้งาน (User) และผู้ดูแลบริหารจัดการระบบ (Administrator)

๕.๒.๒ จัดทำคู่มือการใช้ระบบในการปฏิบัติงานและการปรับปรุงคู่มือให้เป็นปัจจุบัน

๕.๒.๓ จัดฝึกอบรมเสร็จสิ้นครบถ้วนตามหลักสูตรที่บรรจุในแผนการฝึกอบรมเพื่อป้องกันความผิดพลาดที่เกิดขึ้นในการปฏิบัติงานหรือความเสียหายในการใช้ระบบ

๕.๓ ลิขสิทธิ์โปรแกรม

๕.๓.๑ จัดเก็บข้อมูลจำนวน License ของ Software และโปรแกรมระบบงานที่พัฒนาเสร็จสมบูรณ์ทุกระบบงาน (Source Code) ทั้งหมด

๕.๓.๒ มีการปรับปรุงเอกสารให้เป็นปัจจุบัน

๕.๔ ความพร้อมใช้งาน (Availability)

๕.๔.๑ แผนสำรองข้อมูลและระบบงาน (Backup)

- กำหนดระยะเวลาและความถี่ในการสำรองข้อมูลและระบบงาน

๕.๔.๒ แผนกู้คืนข้อมูลทั้งระบบรวมฐานข้อมูล (Recovery) โดยกำหนดระยะเวลาและความถี่ของการทดสอบกู้คืนข้อมูลทั้งระบบรวมทั้งฐานข้อมูล

๕.๕ การบริหารจัดการระบบงาน

๕.๕.๑ ต้องกำหนดหลักการเขียนโค้ด (Secure Coding) อย่างมั่นคงปลอดภัยในการพัฒนาระบบให้มีความมั่นคงปลอดภัย รวมถึงต้องควบคุมและกำหนดสิทธิ์การเข้าถึง Source Code ของระบบงานอย่างเหมาะสม ให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบตามที่ได้รับมอบหมาย

/๕.๕.๒ กำหนดค่า ...

๕.๕.๒ กำหนดค่าข้อมูลพื้นฐานและค่า configuration ต่าง ๆ

๕.๕.๓ มีการสร้างบัญชีผู้ใช้งาน และรหัสผ่านครั้งแรกแก่ผู้ใช้บริการ หรือให้มีการใช้ระบบในการตั้งรหัสผ่านโดยอัตโนมัติ และรหัสผ่านควรยากต่อการคาดเดา สำหรับควบคุมการเข้าใช้งานอย่างถูกต้องและเชื่อถือได้

๕.๕.๔ มีวิธีการสำหรับการระบุตัวตน (Identification) และใช้ในการพิสูจน์ยืนยันตัวตน (Authentication) ที่เคร่งครัด อย่างน้อยต้องมีการกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เหมาะสมเพื่อ Login เข้าใช้ระบบงานตามสิทธิ์และหน้าที่ที่ได้รับมอบหมาย

๕.๕.๕ มีการล็อคบัญชีผู้ใช้งานเมื่อใส่รหัสผ่านไม่ถูกต้องเกินกว่าจำนวนครั้งที่กำหนด

๕.๕.๖ บังคับให้เปลี่ยนชื่อบัญชีผู้ใช้งานและรหัสผ่านเมื่อเข้าสู่ระบบงานครั้งแรก

๕.๕.๗ มีการกำหนดให้ผู้ใช้บริการตั้งค่ารหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษตามแนวปฏิบัติที่ดีในการใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)

๕.๕.๘ มีการแจ้งการเข้าใช้งานครั้งแรกให้ผู้ใช้บริการทราบ ผ่านช่องทาง e-mail หรือ SMS

๕.๕.๙ มีช่องทางที่สะดวกและรวดเร็วในการรับ – แจ้งข่าวสารและปัญหาการใช้ระบบ เช่น แจ้งผ่าน Call Center, Line Official, e-mail, SMS เป็นต้น

๕.๖ การควบคุมระบบงาน Application Control

กำหนดการควบคุมเป็น ๔ ประเภทหลัก ประกอบด้วย

๕.๖.๑ การควบคุมการเข้าถึงระบบข้อมูล

(๑) มีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อเป็นการระบุตัวตนและพิสูจน์ตัวตนจริงของผู้ใช้บริการในขั้นตอนการเข้าใช้ระบบงานด้วยวิธีที่มั่นคงปลอดภัย โดยเลือกใช้วิธีใดวิธีหนึ่งหรือหลายวิธี ดังนี้

(๑.๑) การระบุตัวตนด้วยชื่อบัญชีผู้ใช้งาน (Username) ควบคู่กับรหัสผ่าน (Password)

(๑.๒) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification) เช่น บัตรประจำตัว (ID Card)

(๑.๓) การระบุตัวตนด้วยค่าทางชีวภาพ (Biometric Identification) เช่น ลายนิ้วมือ ใบหน้า

/(๒) มีการกำหนด ...

(๒) มีการกำหนดสิทธิ์ที่เหมาะสมและเพียงพอตามบทบาท ภารกิจและหน้าที่

(๓) มีการบันทึกกิจกรรมต่าง ๆ ในระบบเพื่อการตรวจสอบ (Audit Logging) และใช้เป็นหลักฐานการติดตามตรวจสอบการทำรายการต่าง ๆ ที่เกิดขึ้นในระบบสารสนเทศ

๕.๖.๒ การควบคุมเกี่ยวกับการนำข้อมูลเข้า

(๑) มีระบบการจัดเตรียมข้อมูล ระบบการนำเข้าข้อมูล ระบบการตรวจสอบข้อมูล (Validation) และระบบการ Approve ข้อมูล

(๒) ระบบต้องมีการตรวจสอบข้อมูลที่เข้าสู่ระบบ (Input Validation) โดยอนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบและเงื่อนไขที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลผิดลักษณะ หรือรูปแบบไม่สมเหตุผล หรือผิดตรรกะทางคอมพิวเตอร์ (Logic) และระบบต้องไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลถูกต้อง

(๓) มีหน้าจอสำหรับการตรวจสอบความครบถ้วนของข้อมูลซึ่งอย่างน้อยต้องมีความครบถ้วนของข้อมูลบังคับต้องกรอก (Mandatory Fields) ก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป หากข้อมูลใน Mandatory Field ไม่ถูกต้องครบถ้วน ต้องมีข้อความแจ้งให้ผู้ใช้ทราบทันที และระบบต้องไม่อนุญาตให้ข้ามขั้นตอนนั้นจนกว่าจะกรอกข้อมูลที่ถูกต้องครบถ้วน

(๔) กำหนดลำดับการอนุมัติข้อมูลที่เหมาะสมสำหรับระบบการ Approve ข้อมูล

๕.๖.๓ การควบคุมเกี่ยวกับการประมวลผล

(๑) มีระบบการประมวลผลข้อมูล (Batch Processing)

(๒) ระบบต้องมีการควบคุมการประมวลผลข้อมูล ดังนี้

- มีการสอบทานความถูกต้องของข้อมูลที่ได้มีการบันทึกในระบบก่อนการประมวลผลข้อมูล (Detective Control)
- หากข้อมูลมีความผิดพลาดต้องดำเนินการปรับปรุงแก้ไขก่อนการประมวลผลข้อมูล (Corrective Control)

(๓) ในกรณีที่เกิดความผิดพลาดกับระบบงานระหว่างที่ระบบประมวลผลข้อมูล ให้ระบบมีข้อความแจ้งเตือนผู้ใช้งาน (Error Message) ทราบทันที เพื่อสื่อสารให้เกิดความเข้าใจที่ถูกต้องและต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ รุ่น หรือ Application Path เป็นต้น แต่ควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาดที่สามารถเข้าใจได้เฉพาะบุคลากรที่มีหน้าที่รับผิดชอบเท่านั้น

/(๔) ในกรณี ...

(๔) ในกรณีที่เกิดความผิดพลาดระหว่างการประมวลผลข้อมูล ต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนหน้าได้อย่างถูกต้อง

(๕) มีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบันโดยระบบสามารถดึงข้อมูลจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วน

(๖) มีหน้าจอสรุปข้อมูลการทำรายการเพื่อให้ผู้ใช้ตรวจสอบความถูกต้องและครบถ้วนก่อนทำการยืนยันรายการ

(๗) มีการแสดงผลและรายละเอียดการทำรายการให้ผู้ใช้งานทราบทันทีหลังจากที่ระบบประมวลผลแล้วเสร็จ และมีการจัดเก็บข้อมูลประวัติการทำรายการ (Transaction History) เพื่อให้สามารถทำการตรวจสอบย้อนหลังได้

๕.๖.๔ การควบคุมเกี่ยวกับการนำเสนอข้อมูลออกแสดงผล

(๑) มีระบบการแสดงผลข้อมูล

(๒) กำหนดสิทธิ์ที่เพียงพอในการเข้าระบบการแสดงผลข้อมูล

(๖) การบำรุงรักษาระบบงาน (System Maintenance)

บุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับบุคลากรของสำนักงาน/กอง/กลุ่ม/ศูนย์ ในการพิจารณาการซ่อมบำรุงรักษาระบบงาน กำหนดกระบวนการควบคุมตามขั้นตอนโดยให้มีการดำเนินการและจัดทำเอกสารที่สำคัญ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๖.๑) มีการควบคุมดูแลระบบให้มีความพร้อมใช้งาน (Availability) และเหมาะสมกับการใช้งานในปัจจุบันอย่างต่อเนื่อง ดังนี้

- ตรวจสอบการตั้งค่าระบบ (System Configuration) ให้เหมาะสมกับการใช้งานในปัจจุบัน
- ตรวจสอบขีดความสามารถในการรองรับปริมาณข้อมูลและตรวจสอบความเพียงพอของทรัพยากรระบบ (System Capacity) โดยดำเนินการตามรอบระยะเวลาที่เหมาะสมอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อระบบงาน
- การเปลี่ยนแปลงแก้ไข Patch หรือ Software Update

(๖.๒) มีการบำรุงรักษาระบบงานอย่างต่อเนื่อง

๓๕.๑.๒ มีมาตรการและแนวทางการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management Policy & Procedure) ดังนี้

(๑) ปฏิบัติตามระเบียบวิธีการปฏิบัติในการเปลี่ยนแปลงแก้ไขระบบที่เป็นลายลักษณ์อักษรและมีการอนุมัติจากเจ้าของระบบงาน

(๒) มีการศึกษาผลกระทบต่าง ๆ ทั้งผลกระทบงานด้านเทคนิค ผลกระทบที่มีต่อระบบอื่น และความเสี่ยงจากการเปลี่ยนแปลง

/(๓) บุคลากร ...

(๓) บุคลากรของศูนย์เทคโนโลยีสารสนเทศร่วมกับบุคลากรของสำนักงาน/กอง/กลุ่ม/ศูนย์ หรือมีการแต่งตั้งคณะกรรมการทำหน้าที่กำกับ ดูแล และควบคุมการดำเนินงานในการพัฒนาเปลี่ยนแปลงแก้ไขโปรแกรม และ/หรือ ระบบงาน

(๔) มีการตรวจสอบเอกสารที่เกี่ยวข้องดังนี้

- เอกสารการวิเคราะห์และออกแบบระบบงาน (System Analysis and System Design) ครอบคลุมทุกระบบงาน
- เอกสารแสดง ER Diagram หรือ Flowchart ที่แสดงถึงกระบวนการทำงาน (Procedure) และการไหลของข้อมูล (Data Flow) ของระบบงาน

(๕) มีการควบคุมการเปลี่ยนแปลง Parameter และค่า Configuration ต่าง ๆ โดยการตรวจเช็คความถูกต้องและครบถ้วน

(๖) มีการควบคุมไม่ให้มีการแก้ไขข้อมูลจริงบน Production โดยตรง

(๗) มีการควบคุม Version ของการออกใช้ Software

(๘) มีการทดสอบความถูกต้องและความน่าเชื่อถือของข้อมูลและระบบงานที่แก้ไขแล้วก่อนนำมาใช้งานจริง

(๙) จัดทำเอกสารคู่มือประกอบการแก้ไขเปลี่ยนแปลงทั้งหมด และมีการแก้ไขเอกสารที่เกี่ยวข้อง เช่น คู่มือการใช้งาน คู่มือระบบงาน และข้อมูลเกี่ยวกับการรักษาความปลอดภัยระบบ เป็นต้น

(๑๐) มีการประเมินผลและสอบทานระบบงานหรือโปรแกรมภายหลังจากเริ่มใช้งานในระยะเวลาหนึ่ง

๓๕.๒ กรณีที่ระบบสารสนเทศที่พัฒนาขึ้นใหม่หรือที่ได้รับการปรับปรุงเป็นระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องพิจารณาและกำหนดมาตรการทางเทคนิคในการป้องกันเหตุการณ์อย่างน้อยดังต่อไปนี้

๓๕.๒.๑ การเข้าใช้บริการระบบสารสนเทศโดยไม่ได้รับอนุญาต

๓๕.๒.๒ การแก้ไขระบบสารสนเทศโดยไม่ได้รับอนุญาต

๓๕.๒.๓ การปลอมแปลงสิทธิ์ในการเข้าใช้งานระบบสารสนเทศ

๓๕.๓ กรณีที่ระบบสารสนเทศที่พัฒนาขึ้นใหม่หรือที่ได้รับการปรับปรุงเป็นระบบสารสนเทศที่ให้บริการทางด้านธุรกรรมอิเล็กทรอนิกส์ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องกำหนดมาตรการทางเทคนิคในการป้องกันเหตุการณ์อย่างน้อยดังต่อไปนี้

๓๕.๓.๑ การปลอมแปลงสิทธิ์ในการทำธุรกรรมอิเล็กทรอนิกส์

๓๕.๓.๒ การทำรายการธุรกรรมอิเล็กทรอนิกส์ที่ไม่สมบูรณ์

๓๕.๓.๓ การส่งข้อมูลธุรกรรมอิเล็กทรอนิกส์ที่ผิดพลาด

๓๕.๓.๔ การเข้าถึงข้อมูลธุรกรรมอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

๓๕.๓.๕ การทำสำเนาข้อมูลอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

/๓๕.๔ เจ้าหน้าที่ ...

๓๕.๔ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องควบคุมดูแลให้การเปลี่ยนแปลงที่เกิดขึ้นระหว่างการดำเนินงานพัฒนาระบบอย่างเป็นกระบวนการตามมาตรการที่กำหนด

๓๕.๕ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องควบคุมดูแลไม่ให้มีการเปลี่ยนแปลงแก้ไข Software Package โดยไม่ได้รับอนุญาต และหากจำเป็นต้องแก้ไขให้จำกัดการแก้ไข Software Package นั้น เท่าที่จำเป็น และต้องทำการสำรอง Software Package นั้น ก่อนดำเนินการแก้ไข

๓๕.๖ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องนำหลักการวิศวกรรมสำหรับการพัฒนาระบบให้เกิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการจัดหาและการพัฒนาระบบสารสนเทศ

๓๕.๗. เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้นต้องควบคุมให้การดำเนินงานพัฒนาระบบสารสนเทศอยู่ในบริเวณที่มีความมั่นคงปลอดภัยเพื่อป้องกันความเสี่ยงจากผู้ที่ไม่มีส่วนเกี่ยวข้องกับการพัฒนาระบบเข้าถึงข้อมูล ระบบสนับสนุนและอุปกรณ์เครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาระบบสารสนเทศโดยไม่ได้รับอนุญาต

๓๕.๘ กรณีที่ศูนย์เทคโนโลยีสารสนเทศไม่ได้เป็นผู้พัฒนาระบบสารสนเทศเอง ให้เจ้าหน้าที่ผู้ที่ควบคุมการจัดหา พัฒนาหรือปรับปรุงระบบสารสนเทศนั้น ต้องกำกับและติดตามการดำเนินงานของผู้รับจ้างอย่างเหมาะสมตามกิจกรรมและระยะเวลาที่ถูกกำหนดไว้ในแผนการดำเนินงาน และต้องกำหนดให้มีการระบุลิขสิทธิ์ในการพัฒนาระบบสารสนเทศให้ตกเป็นของ สศค. ในสัญญาจ้างด้วย

๓๖. นโยบายความมั่นคงปลอดภัยด้านบริการที่ได้รับจากผู้ให้บริการ (Supplier Relationships Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมผู้ให้บริการภายนอก (Outsource) กรณีมีการว่าจ้างเหมาผู้ให้บริการภายนอกเข้ามาดำเนินการพัฒนาระบบสารสนเทศ บำรุงรักษาระบบสารสนเทศและระบบเครือข่ายของ สศค. เพื่อป้องกันทรัพย์สินของ สศค. ที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ ตลอดจนรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ได้ทำการตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

๓๖.๑ การคัดเลือกผู้ให้บริการภายนอก

๓๖.๑.๑ กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอก และคัดเลือกผู้ให้บริการภายนอกที่มีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และเป็นที่น่าเชื่อถือ

๓๖.๑.๒ สัญญาต้องระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

/๓๖.๒ การควบคุม ...

๓๖.๒ การควบคุมผู้ให้บริการภายนอก

๓๖.๒.๑ ผู้ให้บริการภายนอกที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของ สศค. ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๓๖.๒.๒ กรณีที่ใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น หากจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าได้ปฏิบัติตามขอบเขตที่ได้กำหนดไว้ โดยให้เจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการภายนอกอย่างใกล้ชิดทั้งในกรณีที่ผู้ให้บริการภายนอกมาปฏิบัติหน้าที่ที่ สศค. (Onsite Service) ให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการภายนอกอย่างละเอียด รวมถึงกรณีการให้บริการในลักษณะ Remote Access และต้องปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล เราเตอร์ (Router) และโมเด็มเราเตอร์ (Modem Router) ทันทีที่ผู้ให้บริการภายนอกดำเนินการให้บริการเสร็จสิ้น

๓๖.๒.๓ การอนุญาตให้ผู้ให้บริการภายนอกเข้าถึงระบบและข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล เราเตอร์ (Router) และโมเด็มเราเตอร์ (Modem Router) ที่ใช้ทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งาน และจะเปิดให้ใช้ได้เมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

๓๖.๒.๔ เพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงานโดยทันทีภายในระยะเวลาที่กำหนดไว้

๓๖.๒.๕ เพิกถอน ลบ หรือเปลี่ยนรหัสผ่านของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

๓๖.๒.๖ ลบหรือเปลี่ยนชื่อของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงานออกจากเอกสารต่าง ๆ ของ สศค. ที่มีชื่อของบุคคลดังกล่าวอยู่ในนั้น

๓๖.๒.๗ กำหนดให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งที่ได้มีการปรับปรุงให้ทันสมัยอยู่เสมอ

๓๖.๒.๘ กำหนดให้ผู้ให้บริการภายนอกรายงานการปฏิบัติงาน ปัญหาต่าง ๆ ที่เกิดขึ้น หรือมีโอกาสที่จะเกิดขึ้นได้พร้อมแนวทางแก้ไข

๓๖.๒.๙ กำหนดขั้นตอนในการตรวจรับงานของผู้ให้บริการภายนอก

๓๖.๓ กำหนดและตกลงเกี่ยวกับความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึงการประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบสารสนเทศของ สศค. โดยมีข้อกำหนดอย่างน้อย ดังต่อไปนี้

/๓๖.๓.๑ ประเภท ...

๓๖.๓.๑ ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการของ สศค. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๓๖.๓.๒ ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของ สศค. จากภัยคุกคามทางไซเบอร์

๓๖.๓.๓ ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๓๖.๓.๔ สศค. สงวนสิทธิ์ในการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการภายนอก

๓๖.๔ การจ้างช่วงจะต้องแจ้งให้ สศค. ได้รับทราบหากผู้รับจ้างมีการดำเนินการในลักษณะดังกล่าวอย่างเป็นลายลักษณ์อักษรและต้องระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วง ทั้งนี้เพื่อป้องกันความเสี่ยงต่าง ๆ อันจะส่งผลกระทบที่สำคัญต่อผลิตภัณฑ์หรือบริการที่นำเสนอไว้ในข้อตกลงกับผู้ให้บริการภายนอก

๓๖.๕ ต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้สอดคล้องกับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้น ๆ เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศและเงื่อนไขที่ได้ระบุไว้ในข้อตกลง รวมถึงการจัดการเหตุละเมิดความมั่นคงปลอดภัย (Information Security Incident) และปัญหาที่เกิดขึ้นอย่างเหมาะสม โดยผู้ประสานงานโครงการต้องเป็นผู้ติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอก

๓๖.๖ การเปลี่ยนแปลงที่เกี่ยวข้องกับบริการที่ได้รับจากผู้ให้บริการภายนอกทั้งในส่วนที่ร้องขอการเปลี่ยนแปลงโดย สศค. เอง และส่วนที่ร้องขอการเปลี่ยนแปลงโดยผู้ให้บริการภายนอก ซึ่งต้องดำเนินการสื่อสารให้ทราบร่วมกันทั้งสองฝ่ายก่อนที่ สศค. พิจารณาดำเนินการเปลี่ยนแปลง

๓๖.๗ การพัฒนาระบบงานและซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๓๖.๗.๑ ให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๓๖.๗.๒ ให้ระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างหรือผู้ให้บริการภายนอก

๓๖.๗.๓ กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๓๖.๗.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๓๖.๗.๕ การสำรองข้อมูลและการกู้คืน

(๑) มีการสำรองข้อมูลจากระบบงานและซอฟต์แวร์ไว้บนสื่อบันทึกที่เหมาะสม

(๒) เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

/๓๗. นโยบาย ...

๓๗. นโยบายการปฏิบัติตามกฎหมาย มาตรฐาน และข้อบังคับ (Compliance Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางปฏิบัติในการป้องกันการละเมิดข้อกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง รวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๓๗.๑ ต้องระบุความต้องการทั้งหมดที่สอดคล้องหรือเกี่ยวข้องกับข้อกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง รวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค. ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างชัดเจนและปรับปรุงให้ทันสมัยอยู่เสมอ

๓๗.๒ เพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของข้อกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง รวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค. ที่ว่าด้วยเรื่องสิทธิ์ในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์ บุคลากรของ สศค. ผู้ให้บริการภายนอก ต้องดำเนินการดังนี้

๓๗.๒.๑ ตรวจสอบและควบคุมไม่ให้มีการละเมิดทรัพย์สินทางปัญญา

๓๗.๒.๒ ไม่คัดลอก แก้ไข ถอดถอนโปรแกรมมาตรฐานต่าง ๆ ที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพาที่ สศค. จัดสรรให้ใช้งาน หรือเครื่องให้บริการ และไม่นำไปให้ผู้อื่นใช้งานแทน

๓๗.๒.๓ ไม่ติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดทรัพย์สินทางปัญญา

๓๗.๒.๔ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ส่วนตัวเพิ่มเติมก่อนได้รับอนุญาต

๓๗.๒.๕ ปฏิบัติตามเงื่อนไขการใช้งานหรือข้อกำหนดที่เกี่ยวข้องกับทรัพย์สินทางปัญญาต่าง ๆ ที่ สศค. หรือผู้ใช้งานมีไว้ใช้งานหรือครอบครอง

๓๗.๒.๖ ห้ามเปลี่ยนแปลง และ/หรือ แก้ไขซอฟต์แวร์สำเร็จรูปที่ สศค. จัดหามาใช้งาน เว้นแต่ได้รับอนุญาตให้เปลี่ยนแปลงแก้ไขได้จากเจ้าของลิขสิทธิ์

๓๗.๒.๗ ไม่นำผลงานของผู้อื่น หรือผลงานใด ๆ ที่มีลิขสิทธิ์มาทำการคัดลอก หรือดัดแปลงก่อนได้รับอนุญาตจากเจ้าของลิขสิทธิ์

๓๗.๒.๘ การจัดซื้อจัดหาเอกสาร ข้อมูล ซอฟต์แวร์ และทรัพย์สินทางปัญญา ต้องจัดซื้อกับผู้ผลิตหรือตัวแทนจำหน่ายที่เชื่อถือได้เท่านั้น

๓๗.๒.๙ เอกสาร ข้อมูล ซอฟต์แวร์ และทรัพย์สินทางปัญญาที่จัดซื้อจัดหาเข้ามาต้องถูกบันทึกลงในทะเบียนทรัพย์สินและจัดเก็บเอกสารระบุสิทธิ์ในการใช้งาน หรือเอกสารในการซื้อขายที่สามารถใช้ยืนยันสิทธิ์ในการใช้งานเอาไว้อย่างครบถ้วน

๓๗.๒.๑๐ ต้องเฝ้าติดตามปริมาณการใช้งาน รูปแบบการใช้งาน และรายละเอียดที่เกี่ยวข้องกับการใช้งานทรัพย์สินทางปัญญาให้เป็นไปตามที่เจ้าของลิขสิทธิ์กำหนด

/๓๗.๒.๑๑ เอกสาร ...

๓๗.๒.๑๑ เอกสาร ข้อมูล ซอฟต์แวร์ และทรัพย์สินทางปัญญาที่บุคลากรของ สศค. และผู้ให้บริการภายนอกสร้างขึ้นเพื่อใช้ประกอบการทำงานให้กับ สศค. ถือเป็นลิขสิทธิ์ของ สศค. ยกเว้นกรณีที่มีการจัดทำข้อตกลงอื่นใดที่ระบุเรื่องลิขสิทธิ์ของทรัพย์สินเหล่านี้

๓๗.๓ ข้อมูลของ สศค. ต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่โดยไม่ได้รับอนุญาต โดยต้องสอดคล้องกับความต้องการของข้อกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง รวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค.

๓๗.๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

๓๗.๔.๑ ต้องปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล

๓๗.๔.๒ ต้องกำหนดวัตถุประสงค์ที่ชัดเจนในการจัดเก็บและใช้งานข้อมูลส่วนบุคคล โดยต้องปฏิบัติตามข้อกฎหมายและข้อกำหนดที่เกี่ยวข้อง รวมถึงต้องแจ้งวัตถุประสงค์ในการจัดเก็บให้เจ้าของข้อมูลทราบ ก่อนดำเนินการจัดเก็บข้อมูลส่วนบุคคล

๓๗.๔.๓ ต้องจัดเก็บเฉพาะข้อมูลส่วนที่จำเป็นในการนำไปใช้งานตามวัตถุประสงค์ในการจัดเก็บที่ได้แจ้งกับเจ้าของข้อมูลเท่านั้น

๓๗.๔.๔ ข้อมูลส่วนบุคคลที่จัดเก็บไว้ต้องถูกนำมาใช้งานตามวัตถุประสงค์ในการจัดเก็บที่ได้แจ้งกับเจ้าของข้อมูลเท่านั้น

๓๗.๔.๕ เจ้าของข้อมูลมีสิทธิ์ในการเปลี่ยนแปลง แก้ไข และยกเลิกการอนุญาตให้ใช้ข้อมูลส่วนบุคคลของตนเอง

๓๗.๔.๖ ข้อมูลส่วนบุคคลที่จัดเก็บไว้ถือเป็นข้อมูลในระดับชั้นลับ (Confidential) ต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมาตรการที่เหมาะสม

๓๗.๕ มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง ข้อกฎหมาย ระเบียบข้อบังคับทั้งหมดที่เกี่ยวข้องรวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค.

๓๗.๖ ต้องมีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ สศค. อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่ส่งผลกระทบกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ สศค.

๓๗.๗ ผู้บังคับบัญชา หรือหัวหน้างานต้องดำเนินการทบทวนความสอดคล้องของการประมวลผลสารสนเทศ และขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเองอย่างสม่ำเสมอ โดยเทียบกับนโยบาย มาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

/๓๗.๘ ต้องจัด ...

๓๗.๘ ต้องจัดให้มีการตรวจสอบระบบเทคโนโลยีสารสนเทศทางเทคนิคครอบคลุมระบบสำคัญทั้งหมดอย่างน้อยปีละ ๑ ครั้ง โดยใช้วิธีการอย่างหนึ่งอย่างใดต่อไปนี้

๓๗.๘.๑ Security Configuration Review โดยทบทวนค่า Configuration ของอุปกรณ์เทียบกับมาตรฐานหรือคำแนะนำที่เป็นที่ยอมรับ

๓๗.๘.๒ Vulnerability Assessment โดยใช้เครื่องมือที่เชื่อถือได้ช่วยตรวจสอบหาช่องโหว่ทางเทคนิคในระบบเทคโนโลยีสารสนเทศ

๓๗.๘.๓ Penetration Test โดยทดสอบเจาะระบบเทคโนโลยีสารสนเทศโดยผู้เชี่ยวชาญ

๓๗.๙ ตรวจสอบระบบเทคโนโลยีสารสนเทศทางเทคนิคต้องดำเนินการโดยผู้ที่มีความเชี่ยวชาญเพียงพอและต้องได้รับอนุญาตก่อนดำเนินการ

๓๗.๑๐ ผลการตรวจสอบระบบเทคโนโลยีสารสนเทศทางเทคนิคถือเป็นข้อมูลในระดับชั้นลับ (Confidential) ต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมาตรการที่เหมาะสม

๓๘. นโยบายการใช้บริการคลาวด์ (Cloud Services Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยในการใช้บริการคลาวด์ รวมถึงปกป้องระบบสารสนเทศและแอปพลิเคชั่นที่มีการจัดเก็บไว้ในระบบคลาวด์ให้มีความมั่นคงปลอดภัยไม่ให้ถูกเข้าถึงได้โดยไม่ได้รับอนุญาต

๓๘.๑ ต้องมีการบริหารจัดการระบบบริการคลาวด์อย่างมั่นคงปลอดภัย

๓๘.๒ ต้องมีการกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศและแอปพลิเคชั่นให้สามารถเข้าถึงได้เฉพาะผู้ที่มีส่วนเกี่ยวข้อง ควรตั้งค่าให้เฉพาะเจาะจง เช่น ผู้ที่มีสิทธิ์แก้ไขข้อมูล ผู้ที่มีสิทธิ์ดูเท่านั้น และผู้ที่ไม่มีสิทธิ์เข้าถึง

๓๘.๓ กำหนดเกณฑ์การคัดเลือกบริการคลาวด์ โดยผู้ให้บริการคลาวด์ต้องมีมาตรการป้องกันความมั่นคงปลอดภัยบนโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ อย่างน้อย ดังนี้

๓๘.๓.๑ ต้องกำหนดให้มีวิธีการพิสูจน์ตัวตนในการเข้าถึงระบบคลาวด์ที่มีความมั่นคงปลอดภัย

๓๘.๓.๒ ต้องมีแนวทางในการรักษาความมั่นคงปลอดภัยให้กับโครงสร้างพื้นฐานของการให้บริการคลาวด์

๓๘.๓.๓ ต้องมีวิธีการบริหารจัดการและแก้ไขช่องโหว่เพื่อให้โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของตนเองมีความมั่นคงปลอดภัยอยู่เสมอ

๓๘.๓.๔ ต้องมีกลไกหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการการเปลี่ยนแปลงที่จำเป็นต้องดำเนินการกับโครงสร้างพื้นฐานของการให้บริการ และต้องดำเนินการแจ้งการเปลี่ยนแปลงใด ๆ ก็ตามที่อาจมีผลกระทบกับ สศค. ให้ได้รับทราบก่อนล่วงหน้า

/๓๘.๓.๕ ต้องมี ...

๓๘.๓.๕ ต้องมีข้อมูลสำหรับการติดต่อเพื่อใช้ในการแจ้งและประสานงานการแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นได้อย่างสะดวกและรวดเร็ว

๓๘.๓.๖ ต้องมีโครงสร้างและทีมสำหรับการเฝ้าระวัง ติดตาม และบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย และประสานงานแจ้งให้ สศค. ได้รับทราบตามความจำเป็นและสอดคล้องตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง ระเบียบข้อบังคับ นโยบายและข้อปฏิบัติที่ สศค. กำหนด

๓๘.๓.๗ กรณีที่ สศค. มีความจำเป็นต้องใช้หลักฐานข้อมูลด้านคอมพิวเตอร์ที่อยู่ในส่วนของผู้ให้บริการคลาวด์ ผู้ให้บริการคลาวด์ต้องช่วยเหลือและมอบหลักฐานข้อมูลดังกล่าวอย่างไม่ชักช้า

๓๘.๔ ต้องกำหนดบทบาทและความรับผิดชอบที่เกี่ยวข้องกับการใช้และการบริหารจัดการบริการคลาวด์

๓๘.๕ มีการควบคุมการรักษาความปลอดภัยสารสนเทศที่ดำเนินการโดยผู้ให้บริการระบบคลาวด์

๓๘.๖ มีการบริหารจัดการการควบคุมส่วนต่อประสาน และการเปลี่ยนแปลงต่าง ๆ ในบริการ เมื่อ สศค. ใช้บริการคลาวด์หลายรายการ

๓๘.๗ กำหนดขั้นตอนในการบริหารจัดการเหตุการณ์การรักษาความปลอดภัยสารสนเทศที่เกิดขึ้นเกี่ยวกับการใช้บริการที่คลาวด์สอดคล้องตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง ระเบียบข้อบังคับ นโยบายและข้อปฏิบัติที่ สศค. กำหนด

๓๘.๘ กำหนดแนวทางสำหรับการติดตาม ทบทวน และประเมินการใช้บริการคลาวด์อย่างต่อเนื่องเพื่อบริหารจัดการความเสี่ยงด้านการรักษาความปลอดภัย

๓๙. นโยบายการบริหารจัดการบันทึก (Records Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางป้องกันบันทึกไม่ให้สูญหาย ถูกทำลาย ปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และ/หรือ ปล่อยออกไปโดยไม่ได้รับอนุญาต

๓๙.๑ กำหนดให้มีการเก็บรักษาบันทึกและกำหนดระยะเวลาในการเก็บบันทึก โดยพิจารณาจากข้อกำหนดของกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง นโยบายและข้อปฏิบัติที่ สศค. กำหนด

๓๙.๒ กำหนดให้มีการดำเนินการกับบันทึกให้เหมาะสมตามระดับชั้นความลับของข้อมูลและสารสนเทศ

๓๙.๓ กระบวนการเก็บบันทึกควรกำหนดให้สามารถเข้าถึง ค้นหา และคืนบันทึกที่จำเป็นตลอดระยะเวลาการเก็บรักษาตามที่ สศค. กำหนด

๓๙.๔ กำหนดการบริหารจัดการกุญแจ มีการเก็บรักษากุญแจเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓๙.๕ พิจารณาขั้นตอนการจัดเก็บและการจัดการ ควรดำเนินการตามข้อแนะนำของเจ้าของผลิตภัณฑ์ รวมถึงพิจารณาการเสื่อมสภาพของสื่อที่ใช้ในการเก็บบันทึก

/๔๐. นโยบาย ...

๔๐. นโยบายการบริหารจัดการช่องโหว่ (Vulnerability Management Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางการบริหารจัดการช่องโหว่ทางเทคนิคอย่างเหมาะสม โดยกำหนดแนวทางในการตรวจสอบและแก้ไขช่องโหว่ทางเทคนิคเพื่อป้องกันสารสนเทศจากช่องโหว่ทางเทคนิค

๔๐.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) หรือจากแหล่งอื่นที่น่าเชื่อถือ เป็นต้น

๔๐.๒ ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของ สศค. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญของ สศค.

๔๐.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

๔๐.๓.๑ การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๔๐.๓.๒ การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๔๐.๓.๓ การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๔๐.๔ การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชั่น (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๔๐.๕ การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing) เพื่อให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๔๐.๖ ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชั่นของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๔๐.๗ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น การเพิ่มโมดูลเสริม การปรับปรุงระบบและการปรับเปลี่ยนเทคโนโลยี เป็นต้น

/๔๐.๘ การทดสอบ ...

๔๐.๘ การทดสอบเจาะระบบและผู้ให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

๔๐.๙ การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของ สศค.

๔๐.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

๔๑. นโยบายการบริหารจัดการการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logging Policy)

<u>วัตถุประสงค์</u>

เพื่อควบคุม ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และติดตามผู้ใช้งานระบบ โดยใช้ข้อมูลจราจรคอมพิวเตอร์ (Log) ซึ่งเป็นวิธีการบันทึกเหตุการณ์ และสร้างหลักฐานในกิจกรรมต่างๆ สามารถนำมาใช้วิเคราะห์และระบุเหตุการณ์ด้านความมั่นคงปลอดภัยต่าง ๆ ที่เกิดขึ้นในระบบ

๔๑.๑ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ให้มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังนี้

๔๑.๑.๑ กำหนดให้ผู้ดูแลระบบเครือข่ายมีหน้าที่ความรับผิดชอบในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ลงบนสื่อเก็บข้อมูลที่มีการรักษาความครบถ้วน ถูกต้อง แท้จริง โดยข้อมูลสามารถระบุถึงตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยกำหนดชั้นความลับในการเข้าถึงเพื่อป้องกันและจำกัดสิทธิ์การเข้าถึงเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ห้ามแก้ไขหรือเปลี่ยนแปลงข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของ สศค. (IT Auditor) หรือบุคคลที่ สศค. มอบหมาย

๔๑.๑.๒ กำหนดให้มีการบันทึกการทำงานของระบบปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบบันทึกการพยายามเข้าสู่ระบบ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๔๑.๑.๓ ห้ามดำเนินการ ลบ ทำลาย หรือแก้ไขข้อมูล Log ที่เก็บรักษาไว้

/๔๑.๒ การป้องกัน ...

๔๑.๒ การป้องกัน Log

๔๑.๒.๑ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๔๑.๒.๒ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔๑.๓ การวิเคราะห์ Log

๔๑.๓.๑ วิเคราะห์ Log ต่าง ๆ จากข้อมูลที่จัดเก็บ เช่น การเข้าใช้งาน พฤติกรรมและกิจกรรมที่ผิดปกติเพื่อตรวจสอบความมั่นคงปลอดภัยของระบบ

๔๑.๓.๒ ติดตามข้อมูลข่าวกรองด้านภัยคุกคามและแนวโน้มการเกิดภัยคุกคามต่าง ๆ ในปัจจุบัน

๔๒. นโยบายการเก็บรักษาและลบทำลายข้อมูล (Data Retention and Disposal Policy)

<u>วัตถุประสงค์</u>

เพื่อป้องกันข้อมูลสารสนเทศที่ใช้ในการดำเนินงานที่มีความละเอียดอ่อน ถูกเข้าถึง เปิดเผยโดยไม่ได้รับอนุญาต และเพื่อให้การดำเนินการกับข้อมูลสารสนเทศมีความสอดคล้องกับข้อกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง รวมถึงนโยบายและขั้นตอนปฏิบัติของ สศค. ว่าด้วยการจัดทำ จัดเก็บ ดูแลรักษาความมั่นคงปลอดภัย รวมถึงการกำหนดระยะเวลาการจัดเก็บ และลบทำลายข้อมูลของ สศค. เมื่อสิ้นสุดระยะเวลาในการจัดเก็บ

๔๒.๑ การจำแนกประเภทของข้อมูล

๔๒.๑.๑ กำหนดประเภทของข้อมูลที่เป็นเจ้าของและใช้งานภายใน สศค.

๔๒.๒ การจัดทำและดูแลรักษาข้อมูล

๔๒.๒.๑ จัดทำและเก็บรักษาข้อมูลไว้เพื่อเป็นหลักฐานยืนยันความสอดคล้องกับความต้องการและการดำเนินงานของ สศค.

๔๒.๒.๒ ต้องจัดทำข้อมูลทั้งในรูปของ Hard Copy หรือ Soft Copy หรือทั้งสองรูปแบบที่สามารถอ่านและทำความเข้าใจได้โดยง่าย

๔๒.๒.๓ ต้องกำหนดมาตรการในการบ่งชี้ข้อมูล จัดเก็บข้อมูล ป้องกันข้อมูล ควบคุมการเข้าถึงข้อมูล กำหนดระยะเวลาการจัดเก็บข้อมูล และการลบทำลายข้อมูล

๔๒.๒.๔ ต้องทำให้ข้อมูลที่ใช้งานสามารถระบุ ID และสามารถบ่งชี้แยกตามเรื่องหรือตามชื่อของข้อมูลได้

๔๒.๓ การดูแลด้านความมั่นคงปลอดภัยของข้อมูล

๔๒.๓.๑ จัดเก็บข้อมูลไว้ตามระยะเวลาการจัดเก็บข้อมูลที่ได้กำหนดไว้

๔๒.๓.๒ จัดเก็บและรักษาข้อมูลไว้ในสถานที่และสภาพแวดล้อมที่มีความปลอดภัย

๔๒.๓.๓ จัดเก็บข้อมูล Hard Copy ไว้ในตู้สำหรับจัดเก็บเอกสารที่มีความแข็งแรงและมั่นคง

๔๒.๓.๔ จัดเก็บข้อมูล Soft Copy อย่างมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

/๔๒.๔ การกำหนด ...

๔๒.๔ การกำหนดระยะเวลาการจัดเก็บข้อมูล

๔๒.๔.๑ กำหนดระยะเวลาขั้นต่ำในการจัดเก็บข้อมูลแต่ละประเภท โดยคำนึงถึงความต้องการของ สศค. และความสอดคล้องกับข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ รวมถึงนโยบายและแนวปฏิบัติที่ สศค. กำหนด

๔๒.๔.๒ เมื่อพ้นระยะเวลาการจัดเก็บที่กำหนดไว้ สศค. สามารถพิจารณาขยายระยะเวลาการจัดเก็บข้อมูลเพิ่มเติมได้ตามความเหมาะสม โดยพิจารณาปฏิบัติให้สอดคล้องกับข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ นโยบายและแนวปฏิบัติที่ สศค. กำหนด รวมถึงมาตรฐาน และข้อบังคับ (Compliance Policy)

๔๒.๕ การลบทำลายข้อมูล

๔๒.๕.๑ พิจารณาลบทำลายข้อมูลสำหรับกรณีดังต่อไปนี้

- ข้อมูลนั้นเกินระยะเวลาการจัดเก็บที่ได้กำหนดไว้
- ข้อมูลนั้นไม่มีความจำเป็นหรือความต้องการใช้งานอีกต่อไป
- ข้อมูลนั้นไม่ได้มีความจำเป็นที่จะต้องนำไปใช้เกี่ยวกับการฟ้องร้องดำเนินคดี หรือถูกนำไปใช้ในการสอบสวน
- ไม่มีกฎหมาย ระเบียบ ข้อบังคับ หรือสัญญาจ้างที่กำหนดให้ต้องจัดเก็บข้อมูลนั้นไว้เพื่อเป็นหลักฐานหรือเพื่อการดำเนินการต่าง ๆ

๔๒.๕.๒ ลบทำลายข้อมูลเมื่อพ้นระยะเวลาการจัดเก็บที่กำหนดไว้หรือไม่มีความจำเป็นต่อการใช้งานตามแนวทางและขั้นตอนปฏิบัติที่ สศค. กำหนด

๔๒.๕.๓ จัดทำบันทึกเพื่อขออนุมัติลบทำลายข้อมูลที่พ้นระยะเวลาการจัดเก็บหรือไม่มีความจำเป็นต่อการใช้งาน

๔๒.๕.๔ การลบทำลายข้อมูลและสื่อบันทึกข้อมูลประเภทต่าง ๆ เพื่อป้องกันข้อมูลรั่วไหลและการนำกลับมาใช้ใหม่ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการลบทำลายข้อมูลและสื่อข้อมูล ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

/๔๓. นโยบาย ...

๔๓. นโยบายการกำหนดค่า Configuration อย่างมั่นคงปลอดภัย

<u>วัตถุประสงค์</u>

เพื่อให้การกำหนดค่า Configuration ของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายของ สศค. มีความมั่นคงปลอดภัยสามารถทำงานได้อย่างถูกต้อง รวมถึงเมื่อมีการเปลี่ยนแปลงการกำหนดค่าเพื่อป้องกันความเสี่ยงต่อข้อมูลสารสนเทศที่เกิดจากอุปกรณ์ปลายทางของผู้ใช้งาน

๔๓.๑ การกำหนดค่า Configuration ของฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายของ สศค. จะต้องมีการจัดเก็บค่า Configuration ไว้อย่างมั่นคงปลอดภัย

๔๓.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังนี้

- สิทธิ์พิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- การแบ่งแยกหน้าที่ (Separation of Duties)
- การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- การลบบัญชีที่ไม่ได้ใช้งาน
- การลบบริการและแอปพลิเคชั่นที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชั่นสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
- การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- การป้องกันมัลแวร์ (Malware)
- การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) เพื่อรักษาความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๔๓.๓ มีการกำหนดสิทธิ์ในการเข้าถึงค่า Configuration เท่าที่จำเป็นและสอดคล้องตามตำแหน่งงาน

๔๓.๔ ต้องมีการทบทวน Configuration อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และทำการอัปเดทเมื่อจำเป็นต้องแก้ไข หรือมีภัยคุกคาม หรือตรวจพบช่องโหว่ใหม่ หรือเมื่อมีการเริ่มต้นใช้งานซอฟต์แวร์หรือฮาร์ดแวร์เวอร์ชั่นใหม่

๔๓.๕ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของ สศค.

๔๓.๖ หากมีการเปลี่ยนแปลงค่า Configuration จะต้องดำเนินการตามนโยบายด้านการบริหารจัดการการเปลี่ยนแปลงแก้ไขระบบ (Change Management Policy & Procedure) เพื่อให้มีการอนุมัติ หรืออนุญาต และมีการตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมด รวมถึงจะต้องจัดเก็บค่า Configuration ไว้อย่างน้อย ๑ เวอร์ชั่น พร้อมจัดเก็บหลักฐานในการเปลี่ยนแปลง

/๔๔. นโยบาย ...

๔๔. นโยบายการป้องกันข้อมูลรั่วไหล

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางในการบริหารจัดการข้อมูล ป้องกันข้อมูลที่มีความสำคัญหรือข้อมูลที่มีความอ่อนไหว ไม่ให้เกิดการรั่วไหล หรือถูกเข้าถึง หรือถูกเปลี่ยนแปลง แก้ไข หรือถูกทำให้ไม่เกิดความพร้อมใช้งาน โดยไม่ได้รับอนุญาต

๔๔.๑ กำหนดระดับชั้นความลับของข้อมูลเพื่อให้สามารถดำเนินการกับข้อมูลได้อย่างเหมาะสม ตามขั้นตอนการจัดชั้นความลับและจัดการข้อมูลและสารสนเทศ (Procedure for Information Classification and Management) ตามนโยบายบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management Policy)

๔๔.๒ กำหนดหมวดหมู่ของรายการข้อมูลทั้งหมดที่ต้องการควบคุมการรั่วไหล โดยข้อมูลแต่ละรายการควรมีการจัดเก็บไว้เป็นหมวดหมู่เพื่อให้ง่ายในการบริหารจัดการข้อมูล

๔๔.๓ กำหนดสิทธิ์การเข้าถึงข้อมูลแต่ละประเภทให้สามารถเข้าถึงข้อมูลได้ตามความจำเป็นและเหมาะสม รวมถึงต้องมีการทบทวนสิทธิ์อย่างสม่ำเสมอ

๔๔.๔ บริหารจัดการช่องโหว่ทางเทคนิค เช่น การอัพเดทแพทช์และการสแกนประเมินความเสี่ยง (Update Patch Vulnerability Assessment Scan) ซึ่งเป็นกระบวนการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์เพื่อตรวจสอบและแก้ไขช่องโหว่ในซอฟต์แวร์หรือระบบคอมพิวเตอร์ เป็นต้น ตามนโยบายการบริหารจัดการช่องโหว่ (Vulnerability Management Policy)

๔๔.๕ เฝ้าระวังและการวิเคราะห์การเข้าใช้งานระบบสารสนเทศ พฤติกรรม และกิจกรรมที่ผิดปกติ เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบ ตามนโยบายการบริหารจัดการการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logging Policy)

๔๔.๖ พิจารณาจัดหาและใช้ซอฟต์แวร์ หรือเครื่องมือที่ใช้ในการป้องกันข้อมูลรั่วไหล โดยซอฟต์แวร์หรือเครื่องมือควรมีคุณสมบัติเฉพาะ อย่างน้อยดังนี้

๔๔.๖.๑ สามารถตรวจจับและป้องกันการรั่วไหลข้อมูลที่สามารถเกิดขึ้นผ่านช่องทางต่าง ๆ อย่างน้อยดังนี้

- จำกัดปริมาณการส่งข้อมูลทางอีเมล
- จำกัดการจับภาพหน้าจอ (Screen Capture) ในระบบที่มีข้อมูลสำคัญ
- จำกัดการพิมพ์ข้อมูลส่วนบุคคลทางเครื่องพิมพ์เอกสาร
- จำกัดการจัดเก็บข้อมูลทาง Port USB

๔๔.๖.๒ สามารถป้องกันการรั่วไหลข้อมูลโดยระบุและจำกัดการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต

๔๔.๖.๓ สามารถแจ้งเตือนและรายงานเหตุการณ์ที่เกี่ยวข้องกับข้อมูลให้ผู้ดูแลระบบทราบเกี่ยวกับความเคลื่อนไหวของข้อมูล

/๔๔.๗ กรณีที่ ...

๔๔.๗ กรณีที่เกิดเหตุข้อมูลรั่วไหล ต้องมีการดำเนินการตามขั้นตอนการจัดการเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ (Procedure for Incident Management) และหากเป็นเหตุข้อมูลส่วนบุคคลรั่วไหล ต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔๔.๘ ผู้ใช้งานข้อมูลที่เป็นความลับ

ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ รวมถึงข้อกำหนดในการรับ – ส่งข้อมูลที่เป็นความลับหรือข้อมูลที่มีความอ่อนไหวสูงให้ดำเนินการผ่านระบบเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ระหว่าง สศค. กับหน่วยงานภายนอก โดยมีข้อปฏิบัติดังนี้

๔๔.๘.๑ พิจารณาใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) เพื่อเพิ่มการรักษาความมั่นคงปลอดภัยของข้อมูลให้เป็นไปตามมาตรฐานสากล โดยใช้อุปกรณ์จัดเก็บที่มีความปลอดภัยสูง ได้แก่ Smart Card, Token, Hardware Security Module : HSM เป็นต้น ร่วมกับใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ที่ออกและรับรองโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority: CA) ที่ได้รับมาตรฐานสากล (Trusted Third-Party Certification Authority) ในการเข้ารหัสข้อมูลที่รับ – ส่งระหว่างกันเพื่อพิสูจน์และยืนยันตัวบุคคลของผู้ส่งและผู้รับข้อมูลอิเล็กทรอนิกส์

๔๔.๘.๒ ผู้ใช้งานข้อมูลที่เป็นความลับต้องปฏิบัติตามระเบียบและเงื่อนไขการขอใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อย่างเคร่งครัด โดยต้องกรอกแบบฟอร์มคำขอใช้ใบรับรองอิเล็กทรอนิกส์พร้อมยื่นหลักฐานยืนยันตัวตน ประกอบด้วย สำเนาบัตรประจำตัวประชาชนของผู้ขอใช้ใบรับรองพร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง กรณีเป็นชาวต่างชาติให้ใช้สำเนาหนังสือเดินทาง (Passport) พร้อมลงลายมือชื่อรับรองสำเนาถูกต้อง

๔๔.๘.๓ กรณีมอบหมายให้บุคคลอื่นทำหน้าที่แทนในการรับ และ/หรือ ส่งข้อมูลจะต้องมีหนังสือมอบอำนาจพร้อมติดอากรแสตมป์ ๓๐ บาท ตามจำนวนผู้รับมอบอำนาจ พร้อมสำเนาบัตรประจำตัวประชาชนของผู้รับมอบอำนาจเพิ่มเติม

๔๔.๘.๔ ผู้ขอใช้ใบรับรองอิเล็กทรอนิกส์ต้องลงนามในแบบตอบรับใบรับรองอิเล็กทรอนิกส์เพื่อเปิดใช้งาน (Activate) หลังจากที่ได้ส่งแบบฟอร์มคำขอใช้ใบรับรองอิเล็กทรอนิกส์และได้รับแบบตอบรับ

/๔๔.๘.๕ ผู้ขอใช้ ...

๔๔.๘.๕ ผู้ขอใช้ใบรับรองอิเล็กทรอนิกส์มีหน้าที่ดูแลและเก็บรักษารหัสลับ (Private Key) ที่บันทึกอยู่ในอุปกรณ์ตามข้อ ๔๔.๘.๑ โดยห้ามมิให้บุคคลอื่นซึ่งไม่มีอำนาจหรือหน้าที่ที่เกี่ยวข้องใช้รหัสลับดังกล่าว และหากกรณี Private Key สูญหายหรือถูกล่วงรู้ไปถึงบุคคลอื่นซึ่งไม่มีอำนาจหรือหน้าที่ที่เกี่ยวข้อง ผู้ขอใช้ใบรับรองอิเล็กทรอนิกส์มีหน้าที่ที่จะต้องแจ้งต่อหน่วยงานรับลงทะเบียนของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์โดยทันที

๔๔.๘.๖ ผู้ขอใบรับรองอิเล็กทรอนิกส์ต้องไม่นำใบรับรองอิเล็กทรอนิกส์ไปใช้ในทางที่ขัดต่อกฎหมายและความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รวมทั้งต้องปฏิบัติตามเอกสารแนวนโยบาย (Certificate Policy: CP) แนวปฏิบัติ (Certification Practice Statement: CPS) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

/หมวดที่ ๔ ...

หมวดที่ ๔
แนวปฏิบัติในการใช้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพา มาใช้งานระบบเทคโนโลยีสารสนเทศ

๔๕. แนวปฏิบัติในการใช้คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพามาใช้งานระบบเทคโนโลยีสารสนเทศ

<u>วัตถุประสงค์</u>

เพื่อกำหนดมาตรการควบคุมการใช้คอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Surface) มาใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งที่ สศค. จัดสรรให้ และสำหรับผู้ที่นำคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคล หรืออุปกรณ์คอมพิวเตอร์อื่นที่สามารถเชื่อมต่อเครือข่ายไร้สายแบบพกพาได้ ตลอดจนเครื่องมือสื่อสารเคลื่อนที่ (Mobile Computing and Teleworking) ซึ่งเป็นการใช้อุปกรณ์ที่นอกเหนือจากที่ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมไว้ให้ เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ สศค. จะต้องปฏิบัติตามข้อกำหนด ดังต่อไปนี้

๔๕.๑. มาตรการควบคุมการใช้งานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาที่ สศค. จัดสรรให้ใช้งาน

๔๕.๑.๑ คอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพา และอุปกรณ์สื่อสารเคลื่อนที่ที่ สศค. จัดสรรให้ใช้งานเป็นทรัพย์สินของ สศค. ดังนั้น ผู้ใช้จึงต้องใช้งานคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของ สศค.

๔๕.๑.๒. ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ที่ได้กำหนดไว้

๔๕.๑.๓ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สศค. ต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และไม่อนุญาตให้นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือบนเครื่องคอมพิวเตอร์อื่นใดที่ไม่ได้อยู่ในความครอบครองของ สศค. รวมถึงห้ามทำการแก้ไขเปลี่ยนแปลง หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔๕.๑.๔ การป้องกันโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ตรวจสอบหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ ได้แก่ Hard Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนด

/๔๕.๑.๕ ศึกษา ...

๔๕.๑.๕ ศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัย มีประสิทธิภาพโดยไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และต้องรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๔๕.๑.๖ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ สศค. เท่านั้น

๔๕.๑.๗ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๔๕.๑.๘ ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์ที่ สศค. จัดสรรให้ตนเองใช้งาน เช่น ล็อคเครื่องคอมพิวเตอร์ขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องคอมพิวเตอร์ทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ไม่เก็บ หรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น หรือฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๔๕.๑.๙ กรณีต้องการเคลื่อนย้ายคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ต้องใส่กระเป๋าสำหรับคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การตกจากโต๊ะทำงาน หรือหลุดมือ

๔๕.๑.๑๐ หลีกเลี่ยงการใช้นิ้ว หรือของแข็ง หรือปลายปากกานำไปสัมผัสหน้าจอ LCD ของคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของ สศค. ซึ่งอาจทำให้หน้าจอแตกหักหรือเสียหายได้

๔๕.๑.๑๑ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๔๕.๑.๑๒ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๔๕.๑.๑๓ หากมีการนำคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ซึ่งไม่ใช่ทรัพย์สินของ สศค. มาใช้กับระบบเครือข่ายของ สศค. ต้องได้รับอนุญาตและตรวจสอบจากศูนย์เทคโนโลยีสารสนเทศก่อนการใช้งาน

๔๕.๑.๑๔ ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานเมื่อใช้งานเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๔๕.๑.๑๕ ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

๔๕.๑.๑๖ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ สศค. ยกเว้นจะได้รับอนุญาตและตรวจสอบจากศูนย์เทคโนโลยีสารสนเทศก่อนการใช้งาน

/๔๕.๒ มาตรการ ...

๔๕.๒ มาตรการควบคุมการใช้งานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลเพื่อรักษาความปลอดภัยระบบเครือข่ายของ สศค. โดยควบคุมการนำอุปกรณ์ส่วนตัวเข้ามาใช้งานบนระบบเครือข่ายของ สศค. (Bring Your Own Device – BYOD) โดยกำหนดให้มีการยืนยันตัวตนและกำหนดสิทธิ์ให้อุปกรณ์ต่าง ๆ มีสิทธิ์ในระดับที่แตกต่างกัน หรือบางกรณีอาจห้ามไม่ให้มีการใช้งานอุปกรณ์บางประเภทที่มีความเสี่ยงทางด้านความปลอดภัยในระดับสูง

๔๕.๒.๑ มีการรักษาความมั่นคงปลอดภัยระดับเครือข่ายด้วย Network Access Control (NAC) โดยติดตั้ง Agent แบบชั่วคราวเพื่อตรวจสอบเชิงลึก หรือไม่ติดตั้ง Agent ก็ได้ โดยให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานของ สศค. และใช้งาน Internet จากภายนอกได้ภายหลังการยืนยันตัวตนแล้ว เช่น ระบบ e-mail, เว็บไซต์ภายใน หรือระบบ Chat

๔๕.๒.๒ ผู้ใช้งานต้องดำเนินการร้องขออนุญาตการใช้งานคอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคล โดยดำเนินการร้องขอต่อเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมาย หรือทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษรอักษร

๔๕.๒.๓ ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศตามสิทธิ์ในการเข้าถึงระบบสารสนเทศที่กำหนดไว้เท่านั้น ในกรณีที่ผู้ใช้งานต้องการเข้าถึงระบบสารสนเทศที่เกินกว่าสิทธิ์ที่ได้รับ ให้ดำเนินการกรอกแบบฟอร์มการบริหารจัดการบัญชีรายชื่อและสิทธิ์ โดยให้หัวหน้างานพิจารณาอนุมัติ

๔๕.๒.๔ ผู้ใช้งานต้องพิสูจน์ยืนยันตัวตนในการเข้าถึงระบบสารสนเทศหรือการเข้าถึงเครือข่ายภายในของ สศค.

๔๕.๒.๕ เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายต้องตรวจสอบการติดตั้งและ Activate ซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี รวมทั้งตรวจสอบการติดตั้งซอฟต์แวร์อันตรายที่ติดตั้งภายในคอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลของผู้ใช้งานก่อน

๔๕.๒.๖ หลังจากได้รับการอนุญาตให้ใช้งาน หากตรวจพบซอฟต์แวร์อันตราย เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายจะดำเนินการถอดถอนซอฟต์แวร์ออกจากคอมพิวเตอร์ของผู้ใช้งาน หรือถอดถอนสิทธิ์การใช้งานคอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพาส่วนบุคคลเครื่องนั้น

๔๕.๒.๗ ผู้ใช้งานต้องติดตั้งโปรแกรมในอุปกรณ์คอมพิวเตอร์ตามที่ สศค. อนุญาตให้ใช้งานได้เท่านั้น หากต้องการติดตั้งโปรแกรมที่นอกเหนือจากที่ สศค. อนุญาตจะต้องทำการร้องขอต่อเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายอย่างชัดเจนเป็นลายลักษณ์อักษร

/๔๕.๒.๘ ผู้ใช้งาน ...

๔๕.๒.๘ ผู้ใช้งานต้องตั้งรหัสผ่านและล็อคหน้าจอทุกครั้งเมื่อไม่ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๔๕.๒.๙ ผู้ใช้งานต้องออกจากระบบและล็อคหน้าจอทุกครั้งเมื่อไม่ใช้งาน

๔๕.๒.๑๐ ในการรับ - ส่งข้อมูลสำคัญผ่านระบบเครือข่าย ผู้ใช้งานต้องดำเนินการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL หรือ XML Encryption เป็นต้น

๔๕.๒.๑๑ ในการจัดเก็บข้อมูลที่มีความสำคัญ ผู้ใช้งานต้องดำเนินการเข้ารหัสข้อมูล

๔๕.๒.๑๒ ผู้ใช้งานต้องไม่นำอุปกรณ์คอมพิวเตอร์แบบพกพาวางทิ้งไว้ในพื้นที่สาธารณะเพื่อป้องกันการสูญหายซึ่งอาจทำให้เกิดข้อมูลรั่วไหล

๔๕.๒.๑๓ เมื่ออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งานสูญหายจะต้องดำเนินแจ้งให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายรับทราบภายใน ๒๔ ชั่วโมง

๔๕.๒.๑๔ เมื่อผู้ใช้งานต้องการยกเลิกการใช้งานหรือลาออก เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายจะต้องดำเนินการลบข้อมูลที่เป็นความลับออกจากคอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งาน

๔๕.๒.๑๕ เมื่อผู้ใช้งานเจอเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศให้ดำเนินการแจ้งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายผ่านช่องทางที่ศูนย์เทคโนโลยีสารสนเทศกำหนด เช่น QR Code หรือแบบฟอร์มการร้องขอ Incident Request เพื่อให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายดำเนินการประเมินความเร่งด่วนของเหตุการณ์และจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น

๔๕.๒.๑๖ ไม่อนุญาตให้นำอุปกรณ์คอมพิวเตอร์แบบพกพาในรูปแบบ Rooted (Android) หรือ jailbroken (iOS) เข้าถึงเครือข่ายและระบบสารสนเทศของ สศค.

๔๕.๒.๑๗ สศค. ขอสงวนสิทธิ์ในการดำเนินการตรวจสอบคอมพิวเตอร์ (PC) หรืออุปกรณ์คอมพิวเตอร์แบบพกพาของผู้ใช้งานและตัดสิทธิ์การใช้งานเมื่อพบเจอสิ่งผิดปกติ

๔๕.๒.๑๘ กรณีที่ต้องเข้าถึงข้อมูลหรือระบบจากระยะไกล (Teleworking) ต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่ สศค. กำหนด รวมถึงมาตรการควบคุมการปฏิบัติงานจากภายนอก สศค.

๔๕.๒.๑๙ ผู้ใช้งานต้องดำเนินการสำรองข้อมูล (Backup) ของตนเอง

๔๕.๒.๒๐ ในการใช้บริการเว็บไซต์และเว็บแอปพลิเคชั่นต่าง ๆ ต้องระมัดระวังในการใช้งานควรเข้าใช้งานในแหล่งที่ปลอดภัยและน่าเชื่อถือเพื่อป้องกันความปลอดภัยของระบบสารสนเทศ

/๔๕.๓ มาตรการ ...

๔๕.๓ มาตรการควบคุมความเสี่ยงจากการใช้อุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและระบบสารสนเทศซึ่งไวต่อการรบกวน

๔๕.๓.๑ ระบบซึ่งไวต่อการรบกวนซึ่งเป็นระบบที่มีผลกระทบและมีความสำคัญสูงต่อ สศค. ได้แก่ ระบบสารสนเทศสถาบันการเงินและสถาบันการเงินเฉพาะกิจซึ่งมีการแลกเปลี่ยนและรับส่งข้อมูลด้านการเงินกับธนาคารแห่งประเทศไทย สถาบันการเงินและสถาบันการเงินเฉพาะกิจตามช่วงระยะเวลาที่กำหนดในบันทึกข้อตกลงความร่วมมือ (MOU) ระหว่าง สศค. และหน่วยงานที่เกี่ยวข้อง เป็นต้น ต้องได้รับการแยกออกจากระบบอื่น ๆ และต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ และหากจำเป็นต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ รวมถึงการปฏิบัติงานจากภายนอก สศค. (Mobile Computing and Teleworking) มีข้อปฏิบัติดังนี้

(๑) มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ห้องปฏิบัติการคอมพิวเตอร์ดังนี้

(๑.๑) กำหนดระเบียบหรือแนวปฏิบัติในการเข้า – ออกพื้นที่ห้องปฏิบัติการคอมพิวเตอร์

(๑.๒) ควบคุมการเข้า - ออก ด้วยระบบรักษาความปลอดภัย เช่น ระบบ Hand Scan ระบบ Finger Print พร้อมระบบ CCTV เป็นต้น

(๑.๓) ติดตั้งระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๔) จัดหาเครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๑.๕) ติดตั้งระบบระบายอากาศ

(๑.๖) ติดตั้งระบบปรับอากาศและควบคุมความชื้น

(๑.๗) ติดตั้งระบบดับเพลิง ระบบตรวจสอบควันไฟและน้ำรั่วซึม

(๒) มีการสำรองข้อมูลและกู้คืนระบบคอมพิวเตอร์ (Backup And Recovery) ระบุไว้ในแผนสำรองข้อมูลและระบบสารสนเทศ

(๓) มีแผนฉุกเฉินกรณีระบบคอมพิวเตอร์ขัดข้องและระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

(๔) มีแผนฉุกเฉินกรณีเกิดอุทกภัย หรือภัยพิบัติทางธรรมชาติและระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

(๕) ระบบที่มีผลกระทบและความสำคัญสูงต่อ สศค. หากต้องมีการใช้งานผ่านคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่าง ๆ ซึ่งมิใช่ทรัพย์สินของ สศค. จะต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

/๔๕.๔ มาตรการ ...

๔๕.๔ มาตรการควบคุมการปฏิบัติงานจากภายนอก สศค. (Teleworking) เพื่อควบคุมการใช้งานระบบต่าง ๆ ที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน สศค. และรักษาความมั่นคงปลอดภัยให้แก่ระบบงานต่าง ๆ จากการเรียกใช้งานจากภายนอก

๔๕.๔.๑ การเข้าถึงระบบงานและข้อมูลจากระยะไกล (Remote Access) เข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของ สศค. อาจก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของ สศค. จึงจำเป็นต้องมีการควบคุมบุคคลที่จะเข้าถึงระบบและข้อมูลของ สศค. จากระยะไกล โดยกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าถึงปกติทั่วไป

๔๕.๔.๒ ต้องกำหนดแนวทาง แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอก สศค.

๔๕.๔.๓ วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงระบบงานและข้อมูลได้จากระยะไกลจะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน โดยกำหนดขั้นตอนการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และต้องปฏิบัติตามข้อกำหนดของการเข้าถึงระบบงานและข้อมูลอย่างเคร่งครัด

๔๕.๔.๔ ก่อนทำการให้สิทธิ์ในการเข้าถึงระบบงานและข้อมูลจากระยะไกล ผู้ประสงค์จะเข้าถึงระบบงานและข้อมูลจากระยะไกลต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ สศค. อย่างเพียงพอและต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือบุคคลที่ได้รับมอบหมาย

๔๕.๔.๕ มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าถึงระบบงานและข้อมูลจากระยะไกลอย่างรัดกุม

๔๕.๔.๖ การอนุญาตให้ผู้ประสงค์จะเข้าถึงระบบงานและข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) อุปกรณ์เชื่อมต่อระยะไกล เราเตอร์ (Router) และโมเด็มเราเตอร์ (Modem Router) ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นหรือไม่มีการใช้งาน ช่องทางดังกล่าวต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

/หมวดที่ ๕ ...

หมวดที่ ๕
แนวปฏิบัติในการรักษาความปลอดภัยข้อมูลส่วนบุคคล สำหรับการใช้งานระบบอินทราเน็ต (Intranet) สศค.

๔๖. แนวปฏิบัติในการรักษาความปลอดภัยข้อมูลส่วนบุคคลสำหรับการใช้งานระบบอินทราเน็ต (Intranet) สศค.

<u>วัตถุประสงค์</u>

สศค. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล โดยมีศูนย์เทคโนโลยีสารสนเทศ (ศทส.) เป็นผู้ดูแลและบริหารจัดการข้อมูลส่วนบุคคล ขอแจ้งให้บุคลากรของ สศค. ซึ่งเป็นผู้ใช้บริการของ สศค. รับทราบถึงวิธีการเก็บรวบรวม ใช้ และเปิดเผย โดยจะปกป้องดูแลข้อมูลส่วนบุคคลของบุคลากรของ สศค. อย่างโปร่งใส เป็นธรรม และเป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายอื่นที่เกี่ยวข้อง

๔๖.๑ ข้อมูลส่วนบุคคลของบุคลากรของ สศค.

๔๖.๑.๑ ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขโทรศัพท์ วันเดือนปีเกิด รูปภาพ รวมถึงข้อมูลทางชีวมิติ (Biometric) เช่น ใบหน้า ลายนิ้วมือ เป็นต้น แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

๔๖.๑.๒ สศค. จะเก็บรวบรวมข้อมูลส่วนบุคคลจากบุคลากรของ สศค. ซึ่งเป็นผู้ให้ข้อมูลนั้นโดยตรงจากการกรอกข้อมูลบนแบบฟอร์มแสดงข้อมูลผู้ขอลงทะเบียนเข้าใช้ระบบอินทราเน็ต (Intranet) และระบบลงเวลา Finger Print และเก็บข้อมูลลายนิ้วมือ ข้อมูลสแกนใบหน้า เป็นต้น โดยเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น และใช้ข้อมูลดังกล่าวตามวัตถุประสงค์ที่กำหนด ซึ่งเป็นวัตถุประสงค์ที่ชอบด้วยกฎหมาย หรือเป็นการดำเนินการตามข้อกำหนดของกฎหมายที่ให้ ศทส. ต้องจัดเก็บข้อมูลดังกล่าว

๔๖.๑.๓ การจัดเก็บข้อมูลอ่อนไหว กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้มีการกำหนดข้อมูลบางประเภทให้เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ ศาสนา พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ความพิการ ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลสุขภาพ เป็นต้น และการเก็บรวบรวมจะทำได้ต้องเป็นไปตามที่กฎหมายกำหนด ซึ่งรวมถึงอาจต้องได้รับความยินยอมจากบุคลากรของ สศค. ดังนั้น สศค. จะดำเนินการเก็บรวบรวมข้อมูลอ่อนไหวเฉพาะในกรณีที่จำเป็นเท่านั้น โดยจะแจ้งให้บุคลากรของ สศค. ทราบอย่างชัดแจ้งถึงเหตุผลความจำเป็น รวมถึงอาจดำเนินการขอความยินยอมจากบุคลากรของ สศค. เพื่อเก็บรวบรวมข้อมูลอ่อนไหวดังกล่าวในบางกรณี

/ข้อมูล ...

ข้อมูลส่วนบุคคลของบุคลากรของ สศค.ที่เก็บรวบรวม มีดังต่อไปนี้

(๑) ข้อมูลส่วนตัว เช่น ชื่อ นามสกุล (ภาษาไทย ภาษาอังกฤษ) หมายเลขบัตรประชาชน วันเดือนปีเกิด กรุ๊ปเลือด สถานะภาพสมรส ศาสนา เป็นต้น

(๒) ข้อมูลการติดต่อ เช่น ภูมิลำเนา ที่อยู่ตามทะเบียนบ้าน ที่อยู่ที่สามารถติดต่อได้ ชื่อบิดามารดา ชื่อคู่สมรส (ถ้ามี) FPO - Mail เป็นต้น

(๓) ข้อมูลเกี่ยวกับงานของบุคลากรของ สศค. เช่น รหัสพนักงาน สังกัด ประเภทบุคลากร วันที่รับราชการ วันที่เข้าส่วนราชการ ตำแหน่ง ระดับตำแหน่ง เงินเดือน (ถ้ามี) เป็นต้น

๔๖.๒ วัตถุประสงค์การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของบุคลากรของ สศค.

สศค. มีความจำเป็นต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคลากรของ สศค. เพื่อวัตถุประสงค์ดังนี้

๔๖.๒.๑ สำหรับใช้ลงทะเบียนการเข้าใช้งานระบบเครือข่ายภายในของ สศค. ที่เรียกว่า ระบบอินทราเน็ต (Intranet) ประกอบด้วยระบบพื้นฐานที่สำคัญต่าง ๆ ของ สศค. ดังนี้

(๑) ระบบบริหารจัดการโครงสร้าง สศค. (Staff Directory)

(๒) ระบบ Active Directory (AD)

(๓) ระบบ FPO Mail

(๔) ระบบลา - ลงเวลาปฏิบัติงาน

(๕) ระบบเครื่องลงเวลา

(๖) ระบบสารบรรณอิเล็กทรอนิกส์

(๗) ระบบจองรถยนต์

(๘) ระบบจองห้องประชุม

(๙) ระบบสลิปเงินเดือน

๔๖.๒.๒ สำหรับประสานและติดต่อให้ความช่วยเหลือในการตอบข้อซักถามหรือให้บริการแก่บุคลากรของ สศค.

๔๖.๒.๓ สำหรับการวิเคราะห์และตรวจสอบเพื่อปรับปรุงการใช้งานหรือการให้บริการ ตลอดจนสนับสนุนการพัฒนานวัตกรรมใหม่เพื่อให้บุคลากรของ สศค.ได้รับความสะดวกสบายที่ดียิ่งขึ้น

๔๖.๒.๔ ปฏิบัติงานตามหน้าที่ที่กฎหมายกำหนด

/๔๖.๓ ฐานกฎหมาย ...

๔๖.๓ ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบุคลากรของ สศค. นั้น จะดำเนินการเท่าที่จำเป็นและเป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดหลักการและเหตุผลทางกฎหมายไว้หลายประการตามสถานการณ์ที่แตกต่างกันซึ่งอนุญาตให้ สศค. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายนี้สามารถดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบุคลากรของ สศค. ได้ ทั้งนี้ สศค. จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบุคลากรของ สศค. เมื่อมีฐานทางกฎหมายรองรับ ดังนี้

๔๖.๓.๑ บุคลากรของ สศค. หรือผู้แทนโดยชอบด้วยกฎหมายของบุคลากรของ สศค. ให้ความยินยอม (แล้วแต่กรณี)

๔๖.๓.๒ เป็นการจำเป็นในการปกป้องหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

๔๖.๓.๓ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของ สศค. หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ สศค.

๔๖.๓.๔ เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของ สศค. หรือของบุคคล หรือนิติบุคคลอื่นเว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิ์ขั้นพื้นฐานในข้อมูลส่วนบุคคลของบุคลากรของ สศค.

๔๖.๓.๕ เป็นการจำเป็นเพื่อปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๔๖.๔ รายละเอียดการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

กำหนดแนวปฏิบัติสำหรับการดำเนินกิจกรรมที่เกี่ยวข้องในการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยแต่ละกิจกรรมและบริการเหล่านั้นจำเป็นต้องมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของบุคลากรของ สศค. โดยมีรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของบุคลากรของ สศค. ดังนี้

๔๖.๔.๑ สร้าง Username และ Password เพื่อเข้าใช้ระบบ Intranet

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- รหัสพนักงาน - สังกัด - ตำแหน่ง - ชื่อ นามสกุล (ภาษาไทย ภาษาอังกฤษ) - ประเภทบุคลากร - เลขประจำตัวประชาชน - วันเดือนปีเกิด - ศาสนา

หัวข้อ		รายละเอียด
		- วันที่รับราชการ - วันที่เข้าส่วนราชการ - ตำแหน่ง - ระดับตำแหน่ง - ที่อยู่ที่สามารถติดต่อได้ - FPO-Mail - User logon name
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	- เพื่อสร้าง Username และ Password ของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่เพื่อให้สามารถเข้าใช้งานระบบ Intranet ได้ - เพื่อยืนยันตัวตนเข้าใช้ระบบ Intranet
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๒ เพิ่มเจ้าหน้าที่หรือบุคลากรของ สศค. ลงในระบบบริหารจัดการโครงสร้าง สศค. (Staff Directory)

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- รหัสพนักงาน - สังกัด - ตำแหน่ง - ชื่อ นามสกุล (ภาษาไทย ภาษาอังกฤษ) - ประเภทบุคลากร - เลขประจำตัวประชาชน - วันเดือนปีเกิด - ศาสนา - วันที่รับราชการ - วันที่เข้าส่วนราชการ - ตำแหน่ง - ระดับตำแหน่ง - ที่อยู่ที่สามารถติดต่อได้ - FPO-Mail - User logon name
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูล	เพื่อเพิ่มข้อมูลของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่ลงในระบบบริหารจัดการโครงสร้าง สศค. (Staff Directory)

หัวข้อ		รายละเอียด
	ส่วนบุคคล	
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๓ สร้าง Username และ Password ในระบบ AD

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- ชื่อ นามสกุล (ภาษาไทย ภาษาอังกฤษ) - เลขประจำตัวประชาชน
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	- เพื่อสร้าง Username และ Password ของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่ลงในระบบ AD - เพื่อยืนยันตัวตนเข้าใช้เครื่องคอมพิวเตอร์ของสศค. และเข้าใช้ระบบเครือข่ายอินเทอร์เน็ตไร้สาย
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๔ สร้าง Accounts และ Password เพื่อเข้าใช้ FPO - Mail

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- ชื่อ นามสกุล (ภาษาไทย ภาษาอังกฤษ) - เลขประจำตัวประชาชน
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	เพื่อสร้าง Accounts และ Password ของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่เพื่อให้สามารถเข้าใช้ FPO - Mail ได้
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๕ เพิ่มเจ้าหน้าที่หรือบุคลากรของ สศค. ลงในระบบลา - ลงเวลา

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้าง	- รหัสพนักงาน

หัวข้อ		รายละเอียด
	ที่มีการเก็บรวบรวม	- สังกัด - ชื่อ นามสกุล (ภาษาไทย) - ประเภทบุคลากร - วันที่รับราชการ - ตำแหน่ง
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	- เพื่อเพิ่มข้อมูลของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่ลงในระบบลา - ลงเวลา - เพื่อยืนยันตัวตนเข้าใช้ระบบลาและใช้สำหรับตรวจสอบเวลาปฏิบัติราชการ
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๖ เก็บลายนิ้วมือและสแกนใบหน้าเพื่อจับคู่กับรหัสพนักงาน

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- รหัสพนักงาน - ชื่อ นามสกุล (ภาษาไทย) - ใบหน้า และลายนิ้วมือ
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	- เพื่อเพิ่มข้อมูลของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่ลงในระบบเครื่องลงเวลา - เพื่อสแกนนิ้วลงเวลาเข้าออกปฏิบัติงาน
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๗ สร้าง Username และ Password เพื่อเข้าใช้ระบบงานสารบรรณ

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- ชื่อ นามสกุล (ภาษาไทย) - User logon จากระบบ AD - สังกัด - FPO - Mail
๒	เหตุผลที่จำเป็นต้องเก็บ	- เพื่อสร้าง Username และ Password ของเจ้าหน้าที่และบุคลากรของ

หัวข้อ		รายละเอียด
	รวบรวม หรือใช้ข้อมูลส่วนบุคคล	สศค. รายใหม่เพื่อให้สามารถเข้าใช้ระบบงานสารบรรณได้ - เพื่อยืนยันตัวตนเข้าใช้ระบบสารบรรณ
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๔.๘ สร้าง Username และ Password เพื่อเข้าดูสลิปเงินเดือน

หัวข้อ		รายละเอียด
๑	ข้อมูลส่วนบุคคลใดบ้างที่มีการเก็บรวบรวม	- ชื่อ นามสกุล (ภาษาไทย) - เลขประจำตัวประชาชน
๒	เหตุผลที่จำเป็นต้องเก็บรวบรวม หรือใช้ข้อมูลส่วนบุคคล	- เพื่อสร้าง Username และ Password ของเจ้าหน้าที่และบุคลากรของ สศค. รายใหม่เพื่อให้สามารถเข้าดูสลิปเงินเดือนได้ - เพื่อยืนยันตัวตนเข้าใช้ระบบสลิปเงินเดือน
๓	มีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่	ข้อมูลถูกใช้เฉพาะ Admin ที่ดูแลระบบเท่านั้น
๔	ระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลจะมีการจัดเก็บตามระยะเวลาเท่าที่จำเป็น เมื่อมีคำสั่งลาออก โอน ย้าย ศทส. จะลบ ทำลาย เอกสาร หรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถระบุตัวบุคคลได้

๔๖.๕ สิทธิ์ของบุคลากรของ สศค. ในข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิ์ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และ สศค. ให้ความสำคัญอย่างยิ่งในการดูแลและอำนวยความสะดวกแก่บุคลากรของ สศค. ในฐานะเจ้าของข้อมูลในการดำเนินการตามสิทธิ์เหล่านั้น ดังนี้

๔๖.๕.๑ สิทธิ์ในการได้รับแจ้ง

สศค. จะแจ้ง “นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ สศค.” และ “มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของ สศค.” ที่มีรายละเอียดวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยที่ชัดเจน

๔๖.๕.๒ สิทธิ์ในการเพิกถอนความยินยอม

บุคลากรของ สศค. สามารถขอเพิกถอนความยินยอมที่เคยให้ไว้ได้ทุกเมื่อ โดยสิทธิ์ดังกล่าวรวมถึงข้อมูลส่วนบุคคลของบุคลากรของ สศค. ที่ สศค. ได้เก็บรวบรวมไว้ก่อนที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้

/๔๖.๕.๓ สิทธิ์ ...

๔๖.๕.๓ สิทธิ์ในการเข้าถึงข้อมูล

บุคลากรของ สศค. สามารถขอเข้าถึงข้อมูลส่วนบุคคลของตน และขอสำเนาข้อมูลส่วนบุคคลของตน ตลอดจนสามารถขอให้เปิดเผยการได้มาซึ่งข้อมูลดังกล่าวได้ ทั้งนี้ ในบางกรณี สศค. อาจปฏิเสธคำขอใช้สิทธิ์ข้างต้นได้ หากมีเหตุอันชอบธรรมด้วยกฎหมาย หรือเป็นการดำเนินการใด ๆ เพื่อวัตถุประสงค์ หรือเป็นกรณีที่ต้องปฏิบัติตามกฎหมายหรือคำสั่งศาล หรือเป็นกรณีที่อาจส่งผลกระทบและก่อให้เกิดความเสียหายต่อสิทธิ์หรือเสรีภาพของเจ้าของข้อมูลหรือบุคคลอื่น

๔๖.๕.๔ สิทธิ์ในการแก้ไขข้อมูล

บุคลากรของ สศค. สามารถขอปรับปรุงแก้ไขข้อมูลส่วนบุคคลของตนที่ไม่ถูกต้องได้ เพื่อให้ข้อมูลดังกล่าวมีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด

๔๖.๕.๕ สิทธิ์ในการลบข้อมูล

บุคลากรของ สศค. สามารถขอให้ ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลของตนเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้

๔๖.๕.๖ สิทธิ์ในการโอนข้อมูล

ในกรณีที่ระบบข้อมูลของ สศค. รองรับการอ่านหรือใช้งานโดยทั่วไปด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานอัตโนมัติ และสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ บุคลากรของ สศค. สามารถขอรับสำเนาข้อมูลส่วนบุคคลของตนได้ รวมถึงขอให้มีการโอนถ่ายข้อมูลดังกล่าวไปยังผู้ควบคุมข้อมูลอื่นโดยอัตโนมัติได้ และขอรับข้อมูลส่วนบุคคลที่มีการส่งหรือโอนดังกล่าวได้

๔๖.๕.๗ สิทธิ์ในการระงับการใช้ข้อมูล

บุคลากรของ สศค. สามารถขอให้ระงับการใช้ข้อมูลส่วนบุคคลของตนได้

๔๖.๕.๘ สิทธิ์ในการคัดค้านการประมวลผลข้อมูล

บุคลากรของ สศค. สามารถขอคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนได้

๔๖.๕.๙ สิทธิ์ในการร้องเรียน

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายหรือประกาศที่ออกตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

/๔๖.๖ การรักษา ...

๔๖.๖ การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

สศค. ตระหนักถึงความไว้วางใจของบุคลากรของ สศค. ที่ได้ให้ข้อมูลที่สำคัญกับ สศค. และโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ สศค. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จึงได้ออกประกาศ สศค. เรื่อง นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๗ และ ประกาศ สศค. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๘ เพื่อให้มั่นใจว่าข้อมูลเหล่านั้นจะได้รับการปกป้องดูแลและพร้อมให้เจ้าของข้อมูลเข้าถึงและตรวจสอบ มีแนวทางปฏิบัติ เช่น

๔๖.๖.๑ กำหนดมาตรการป้องกันทางกายภาพและการจำกัดการเข้าถึงข้อมูลส่วนบุคคลไว้เฉพาะเจ้าหน้าที่ของ ศทส. และผู้ดูแลระบบที่มีความจำเป็นต้องเข้าถึงข้อมูลนั้น ๆ

๔๖.๖.๒ กำหนดมาตรการป้องกันการเข้าถึงระบบและข้อมูล เช่น การใช้รหัสผ่านเพื่อเข้าสู่ระบบการให้บริการ เป็นต้น เพื่อป้องกันมิให้ผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลของบุคลากรของ สศค.

๔๖.๖.๓ กำหนดกระบวนการทำงานในการคุ้มครองข้อมูลส่วนบุคคลและการรับมือกับปัญหาหรือเหตุอันน่าสงสัยว่าจะมีการละเมิดข้อมูลส่วนบุคคล โดยหากเกิดเหตุดังกล่าว ศทส. จะรีบแจ้งให้บุคลากรของ สศค. ทราบโดยเร็ว รวมถึงแจ้งเจ้าหน้าที่ที่ดูแลเรื่องนี้ในกรณีที่กฎหมายกำหนดให้ต้องแจ้ง

๔๖.๖.๔ มีการอบรมเจ้าหน้าที่ของ ศทส. เพื่อสร้างความตระหนักและความเข้าใจในขั้นตอนการปฏิบัติงานในการดูแลคุ้มครองข้อมูลส่วนบุคคลและการรับมือกับปัญหาหรือเหตุอันน่าสงสัยว่าจะมีการละเมิดข้อมูลส่วนบุคคล

๔๖.๖.๕ ทบทวนกระบวนการทำงานในการคุ้มครองข้อมูลส่วนบุคคลตามระยะเวลาที่กำหนดเพื่อให้มั่นใจว่ากระบวนการทำงานเป็นไปอย่างเหมาะสมและสอดคล้องกับสถานการณ์ปัจจุบัน

๔๖.๖.๖ ตรวจสอบทดสอบระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลเพื่อให้มั่นใจว่าระบบหรือเทคโนโลยีที่ใช้มีความมั่นคงปลอดภัย รวมถึงการปรับปรุงและติดตั้งซอฟต์แวร์การจัดการด้านการรักษาความมั่นคงปลอดภัยเวอร์ชั่นล่าสุด

อย่างไรก็ตาม บุคลากรของ สศค. ควรตระหนักว่า การส่งข้อมูลผ่านระบบเครือข่ายสาธารณะหรือการใช้เครื่องคอมพิวเตอร์สาธารณะ หรือแม้แต่การใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารส่วนตัวของบุคลากรของ สศค. ที่ติดมัลแวร์ มีความเสี่ยง และเนื่องจากอยู่นอกเหนือ

/การควบคุม ...

การควบคุมและการบริหารจัดการของ ศทส. กรณีดังกล่าว ศทส. ไม่สามารถรับประกันความปลอดภัยในข้อมูลของบุคลากรของ สศค. ซึ่งอาจถูกลักลอบเข้าถึง หรือถูกเปิดเผย หรือถูกโอนถ่ายออกไป และทำให้บุคลากรของ สศค. เกิดความเสียหายได้

๔๖.๗ ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

สศค. จะจัดเก็บข้อมูลส่วนบุคคลของบุคลากรของ สศค. ตามระยะเวลาเท่าที่จำเป็น เพื่อการปฏิบัติหน้าที่และการให้บริการภายใต้วัตถุประสงค์โดยชอบด้วยกฎหมาย โดยระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลอาจมีความแตกต่างกันตามประเภทของกิจกรรมและบริการ

อย่างไรก็ดี สศค. อาจจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลของบุคลากรของ สศค. เกินระยะเวลาที่กำหนดข้างต้น หากมีเหตุที่ สศค. ได้รับแจ้งหรือเชื่อโดยสุจริตได้ว่าอาจมีการกระทำละเมิดข้อตกลงการใช้บริการของ สศค. หรือมีการกระทำฝ่าฝืนกฎหมาย หรือเกิดข้อพิพาท และจำเป็นต้องมีการสืบสวน สอบสวน ตลอดจนรวบรวมหลักฐานเพื่อดำเนินคดีตามกฎหมาย โดย สศค. จะจัดเก็บข้อมูลส่วนบุคคลของบุคลากรของ สศค. ตามระยะเวลาเท่าที่จำเป็นจนกว่ากระบวนการจะเสร็จสิ้น หรือตามระยะเวลาที่กฎหมายที่เกี่ยวข้องในเรื่องนั้นกำหนด

๔๖.๘ การทบทวนและปรับปรุงมาตรการ

สศค. จะทบทวนและปรับปรุงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ สศค. และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของ สศค. เป็นครั้งคราว เพื่อให้แน่ใจว่าเนื้อหาจะมีความเหมาะสม เป็นปัจจุบันและสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายที่เกี่ยวข้อง หากมีการทบทวนและปรับปรุงแก้ไขนโยบายและมาตรการดังกล่าว สศค. จะแจ้งให้บุคลากรของ สศค. ทราบผ่านช่องทางต่าง ๆ ตามความเหมาะสม สศค. ขอแนะนำให้บุคลากรของ สศค. เข้ามาอ่านและตรวจสอบนโยบายและมาตรการอย่างสม่ำเสมอ

ทั้งนี้ หากบุคลากรของ สศค. ยังคงใช้บริการของ สศค. ภายหลังจากที่มาตรการนี้มีการปรับปรุงแก้ไขและได้มีแจ้งให้ทราบแล้ว ถือว่าบุคลากรของ สศค. เห็นชอบและยอมรับในนโยบายและมาตรการที่ได้ปรับปรุงแล้ว

/หมวดที่ ๖ ...

หมวดที่ ๖

แนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔๗ แนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศเพื่อป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๔๗.๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยดังนี้

๔๗.๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๔๗.๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของ สศค. (Internal Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของ สศค.

๔๗.๒ แนวทางในการตรวจสอบและประเมินความเสี่ยง ต้องดำเนินการอย่างน้อยดังนี้

๔๗.๒.๑ ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๔๗.๒.๒ ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔๗.๒.๓ ตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

(๑) จัดลำดับความสำคัญของความเสี่ยง

(๒) ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

(๓) ข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

(๔) สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๔๗.๒.๔ การตรวจสอบและประเมินการรักษาความมั่นคงปลอดภัยให้ครอบคลุมหัวข้ออย่างน้อยต่อไปนี้

(๑) ตรวจสอบและประเมินด้านการบริหารสินทรัพย์ด้านเทคโนโลยีสารสนเทศ

(๒) ตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม

(๓) ตรวจสอบและประเมินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลและการปฏิบัติการ

(๔) การตรวจสอบและประเมินการควบคุมการเข้าถึง

(๕) การตรวจสอบและประเมินการพัฒนาระบบ จัดซื้อจัดหาระบบ และการดูแลรักษาระบบ

(๖) การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์

/๔๗.๒.๕ มีมาตรการ ...

๔๗.๒.๕ มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อยดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๔๗.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๔๗.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log ที่แสดงการเข้าถึงนั้นซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๔๗.๕ กรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต
